

# **Secure Remote Maintenance**

## **User's manual**

Version: **2.00 (September 2023)**

Order no.: **MASRM-ENG**

**Translation of the original manual**



**Publishing information**

B&R Industrial Automation GmbH

B&R Strasse 1

5142 Eggelsberg

Austria

Telephone: +43 7748 6586-0

Fax: +43 7748 6586-26

[office@br-automation.com](mailto:office@br-automation.com)

**Disclaimer**

All information in this document is current as of its creation. The contents of this document are subject to change without notice. B&R Industrial Automation GmbH assumes unlimited liability in particular for technical or editorial errors in this document only (i) in the event of gross negligence or (ii) for culpably inflicted personal injury. Beyond that, liability is excluded to the extent permitted by law. Liability in cases in which the law stipulates mandatory unlimited liability (such as product liability) remains unaffected. Liability for indirect damage, consequential damage, business interruption, loss of profit or loss of information and data is excluded, in particular for damage that is directly or indirectly attributable to the delivery, performance and use of this material.

B&R Industrial Automation GmbH notes that the software and hardware designations and brand names of the respective companies used in this document are subject to general trademark, brand or patent protection.

Hardware and software from third-party suppliers referenced in this document is subject exclusively to the respective terms of use of these third-party providers. B&R Industrial Automation GmbH assumes no liability in this regard. Any recommendations made by B&R Industrial Automation GmbH are not contractual content, but merely non-binding information for which no liability is assumed. When using hardware and software from third-party suppliers, the relevant user documentation of these third-party suppliers must additionally be consulted and, in particular, the safety guidelines and technical specifications contained therein must be observed. The compatibility of the products from B&R Industrial Automation GmbH described in this document with hardware and software from third-party suppliers is not contractual content unless this has been separately agreed in individual cases; in this respect, warranty for such compatibility is excluded in any case, and it is the sole responsibility of the customer to verify this compatibility in advance.

<b>1 General information.....</b>	<b>7</b>
1.1 Manual history.....	7
1.2 Safety guidelines.....	9
1.2.1 Organization of notices.....	9
1.2.2 Introduction.....	9
1.2.3 Intended use.....	9
1.2.4 Protection against electrostatic discharge.....	9
1.2.4.1 Packaging.....	9
1.2.4.2 Regulations for proper ESD handling.....	10
1.2.5 Transport and storage.....	10
1.2.6 Operation.....	10
1.2.6.1 Protection against touching electrical parts.....	10
1.2.6.2 Ambient conditions - Dust, moisture, aggressive gases.....	11
1.2.6.3 Programs, viruses and malicious programs.....	11
1.2.7 Environmentally friendly disposal.....	11
1.2.7.1 Separation of materials.....	11
<b>2 Secure Remote Maintenance.....</b>	<b>12</b>
<b>3 System overview.....</b>	<b>14</b>
3.1 GateManager.....	15
3.1.1 Order data.....	15
3.1.2 Activating the GateManager.....	16
3.1.2.1 Delivery and installation of licenses.....	17
3.1.3 Service fee.....	17
3.1.3.1 Order data.....	17
3.1.4 Additional services.....	17
3.1.4.1 LogTunnel - Remote data logging.....	17
3.1.4.2 SMS license.....	17
3.1.5 User authorization management.....	18
3.1.5.1 GateManager server administrator.....	18
3.1.5.2 GateManager domain administrator.....	18
3.1.5.3 LinkManager user.....	19
3.1.5.4 LinkManager Mobile users.....	19
3.1.5.5 Domain observer.....	19
3.2 SiteManager.....	20
3.2.1 Model comparison.....	20
3.2.2 Order data.....	21
3.2.2.1 SiteManager Embedded.....	21
3.2.2.2 SiteManager hardware.....	21
3.2.3 Technical data.....	23
3.2.3.1 SiteManager Embedded.....	23
3.2.3.2 SiteManager hardware (0RMSM13x5).....	23
3.2.4 Accessories.....	25
3.2.4.1 Terminal blocks.....	25
3.2.4.2 Antennas.....	25
3.2.5 LED status indicators.....	26
3.2.6 Operating and connection elements.....	27
3.2.6.1 Reset button.....	27
3.2.6.2 SD card slot.....	27
3.2.6.3 USB interface.....	27
3.2.6.4 Serial interface.....	27
3.2.6.5 Ethernet interfaces (DEV1/2/3 and UPLINK1).....	28
3.2.6.6 Power supply.....	28
3.2.6.7 I/O interfaces.....	29
3.2.7 Installation.....	30
3.2.8 Initial configuration via controller.....	31



3.2.8.1 Ethernet configuration.....	31
3.2.9 SiteManager_1315-1335-1345 - Initial setup.....	32
3.2.9.1 Configuring UPLINK settings for internet access.....	32
3.2.9.2 Settings for GateManager server connection.....	33
3.2.9.3 Internet access with integrated broadband.....	33
3.2.9.4 Internet access with integrated Wi-Fi module.....	34
3.2.10 Automation Studio.....	35
3.2.10.1 Function model "Standard".....	35
3.2.10.2 Operating function model "Standard".....	39
3.2.11 Connecting to the GateManager.....	40
3.3 LinkManager.....	41
3.3.1 Order data.....	41
3.4 Starter package.....	42
3.4.1 Order data.....	42
3.5 Network safety.....	43
3.6 Port information.....	43
<b>4 Getting started with the system components.....</b>	<b>44</b>
<b>5 Migrating to a new SiteManager version.....</b>	<b>47</b>
5.1 Products.....	47
5.2 Scenarios.....	47
5.2.1 Designing new machines.....	47
5.2.1.1 Steps for the new configuration.....	47
5.2.2 Modifying existing machines.....	47
5.2.2.1 Steps for modifying the existing configuration.....	47
5.2.3 Servicing existing systems.....	47
5.2.3.1 Steps for modifying the existing plant.....	48
<b>6 SiteManager 4G global SIM card Guideline for USA and Japan.....</b>	<b>49</b>
6.1 Affected material.....	49
6.2 Problem statement and resolution.....	49
6.2.1 United States.....	49
6.2.1.1 Verizon.....	49
6.2.1.2 AT&T.....	49
6.2.1.3 T-Mobile.....	50
6.2.2 Japan.....	50
<b>7 Additional documentation.....</b>	<b>51</b>
<b>8 Use cases and end customer scenarios.....</b>	<b>52</b>
8.1 Use cases.....	52
8.1.1 Remote maintenance - On-demand access for programming and trouble-shooting.....	52
8.1.2 Remote monitoring - Secure data logging (between 2 SiteManagers).....	52
8.1.3 Remote monitoring - For secure data logging.....	53
8.1.4 Direct Internet access - For data logging and video surveillance.....	53
8.2 End customer scenarios.....	54
8.2.1 SiteManager and machine in an isolated network.....	55
8.2.2 Machine network isolated behind DMZ and SiteManager.....	56
8.2.3 SiteManager isolated in a separate DMZ.....	56
8.2.4 SiteManager and machine in separate networks.....	57
8.2.5 Remote maintenance - Complete scenario.....	58
8.3 Establishing a connection with FTP.....	59
8.3.1 FTP via SiteManager.....	59
8.3.2 Settings in SiteManager.....	61
8.3.3 Creating a connection with WinSCP.....	62

<b>9 Error correction.....</b>	<b>63</b>
9.1 Testing GateManager access from a PC.....	63
9.2 Connection from PC possible, but not from SiteManager.....	64
9.2.1 Basic questions.....	64
9.2.2 Web proxy issues.....	65
9.2.3 Other possibilities.....	66
<b>10 Standards and certifications.....</b>	<b>67</b>
<b>11 Terminology and abbreviations.....</b>	<b>68</b>
<b>12 Appendix - Discontinued modules.....</b>	<b>69</b>
12.1 GateManager - ORMGM.4260-TP.....	69
12.1.1 Technical data.....	69
12.1.2 LED status indicators.....	70
12.1.3 Operating and connection elements.....	70
12.1.3.1 Reset button.....	70
12.1.3.2 Ethernet interfaces.....	70
12.1.3.3 USB interfaces.....	70
12.1.3.4 Power supply.....	70
12.2 SiteManager 0RMSM 11x5.....	71
12.2.1 SiteManager 11x5.....	71
12.2.1.1 Technical data.....	71
12.2.2 SiteManager 4G - Regional variants.....	72

# 1 General information

## Information:

B&R makes every effort to keep documents as current as possible. The most current versions are available for download on the B&R website ([www.br-automation.com](http://www.br-automation.com)).

## 1.1 Manual history

Version	Date	Comment
2.00	September 2023	<ul style="list-style-type: none"> <li>Added new models 0RMSM1315, 1335.4G and 1345 in section "SiteManager".</li> <li>Moved technical data for SiteManager 0RMSM 11x5 models to appendix and removed other references.</li> <li>Replaced SiteManager image with new version throughout document.</li> <li>Added new sections "SD card slot", "USB interface" and "Serial interface" under "Operating and connection elements".</li> <li>Added new section "Model comparison".</li> <li>Added new section "Connecting to the GateManager".</li> <li>Revised section "SiteManager 13x5 - Initial setup".</li> <li>Revised section "Migrating to a new SiteManager version".</li> <li>Added new section "Error correction".</li> <li>Adjusted order numbers in section "Starter package".</li> <li>Revised section "Port information".</li> </ul>
1.65	April 2022	<ul style="list-style-type: none"> <li>Added information about maximum email sizes in section "GateManager".</li> <li>Added diagram with position of the reset button in section "Operating and connection elements".</li> <li>Added order data for service fees and additional services.</li> <li>Added port information for SiteManager and LinkManager.</li> <li>Added information about downloads to "Getting started with the system components".</li> <li>Added new section "SIM guidelines".</li> <li>Renamed "Solution models" to "Use cases" in section "Use cases and end customer scenarios".</li> </ul>
1.60	August 2021	<ul style="list-style-type: none"> <li>Added new section "Instructions for migrating to SiteManager 4G Global".</li> <li>Moved SiteManager 4G local variants to appendix.</li> </ul>
1.56	May 2021	<ul style="list-style-type: none"> <li>Moved publishing information and changed disclaimer.</li> <li>Added new SiteManager 0RMSM1135-4G.</li> <li>Updated frequency bands in SiteManager technical data.</li> </ul>
1.55	April 2021	<ul style="list-style-type: none"> <li>Moved information about 0RMGM.4260-TP to appendix.</li> <li>Added information about using Verizon SIM cards for the SiteManager.</li> <li>Revised links to GateManager documentation and changed information to LinkManager 7 in section "Getting started with the system components".</li> <li>Changed section "Standards and certifications".</li> <li>New section "Appendix".</li> </ul>
1.50	November 2020	<ul style="list-style-type: none"> <li>Renamed section "Service agreements" to "Service fee" and updated information.</li> <li>Added section "Additional services".</li> <li>Added information about the hypervisor to section "SiteManager - General information".</li> <li>Added danger notice to section "Remote maintenance".</li> <li>Changed section "Standards and certifications".</li> </ul>
1.40	September 2018	<ul style="list-style-type: none"> <li>Section "Installation": Updated to include minimum distances in the control cabinet</li> <li>Combined sections "Solution models" and "End customer scenarios".</li> <li>New section "Establishing a connection with FTP."</li> <li>Editorial changes</li> </ul>
1.32	December 2017	<ul style="list-style-type: none"> <li>New SiteManager hardware module 0RMSM1135.4G-JP.</li> </ul>
1.31	June 2017	<ul style="list-style-type: none"> <li>Renamed EasyLogging to LogTunnel.</li> <li>Updated description of SiteManager LEDs.</li> <li>Section "SiteManager": Divided "Order data" into "Embedded" and "Hardware". Updated order data to include optional accessories and content of delivery.</li> <li>Section "SiteManager": Divided "Technical data" into "Embedded" and "Hardware". Added technical data for SiteManager Embedded.</li> <li>Updated section "Additional documentation".</li> <li>Editorial changes</li> </ul>

## General information

Version	Date	Comment
1.30	March 2017	<ul style="list-style-type: none"> <li>Updated section "Secure Remote Maintenance" with new device models. Highlighted standalone B&amp;R solution as compared to Secomea.</li> <li>Updated section "System overview" to include a minimum system design.</li> <li>Section "GateManager": Updated "General information" to include AWS support and GateManager hosting service.</li> <li>Section "Service agreements": Added 3 new service levels and LogTunnel option.</li> <li>Section "SiteManager": Updated "General information", "Order data" and "Technical data". New SiteManager hardware module with 4G/LTE support and SiteManager Embedded.</li> <li>New section "Accessories": Antennas for mobile network and Wi-Fi.</li> <li>Updated section "Automation Studio" to include I/O mapping register overview and other register descriptions.</li> <li>New section "Starter Package": Faster entry for new customers without high installation costs.</li> <li>Section "Additional documentation" with new grouping of remote data logging.</li> <li>Editorial changes</li> </ul>
1.20	October 2016	<ul style="list-style-type: none"> <li>Replaced section "SiteManager" with data sheet "SiteManager".</li> <li>Updated chapter structure of the included data sheets.</li> <li>Added section "Reset button" for SiteManager.</li> <li>Added contents of SiteManager information sheet to data sheet "SiteManager".</li> <li>Added contents of GateManager information sheet to section "GateManager".</li> <li>Updated section "Additional documentation" to include LogTunnel.</li> <li>Updated description of the main configuration entries (Wi-Fi key mandatory, etc.).</li> <li>Moved parameter table of the main configuration to section "Function model 'Standard'".</li> <li>Updated and reorganized section "Standards and certifications".</li> <li>Added section "Terms and abbreviations".</li> <li>Editorial changes</li> </ul>
1.11a	June 2016	<ul style="list-style-type: none"> <li>Added section "Delivery and installation of licenses".</li> </ul>
1.11		<ul style="list-style-type: none"> <li>Renamed "Installation" to "Commissioning and updated section "Getting started".</li> <li>Updated additional documentation with further notes and explanations regarding the listed vendor documents.</li> <li>Editorial changes</li> </ul>
1.10	March 2016	<ul style="list-style-type: none"> <li>Modified chapter structure.</li> <li>Updated system overview and device overviews.</li> <li>Added end customer scenarios / use cases.</li> <li>Updated link list of associated vendor documents.</li> <li>Editorial changes</li> </ul>
1.00	February 2016	First edition

## 1.2 Safety guidelines

### 1.2.1 Organization of notices

#### Safety notices

Contain **only** information that warns of dangerous functions or situations.

Signal word	Description
<b>Danger!</b>	Failure to observe these safety guidelines and notices will result in death, severe injury or substantial damage to property.
<b>Warning!</b>	Failure to observe these safety guidelines and notices can result in death, severe injury or substantial damage to property.
<b>Caution!</b>	Failure to observe these safety guidelines and notices can result in minor injury or damage to property.
<b>Notice!</b>	Failure to observe these safety guidelines and notices can result in damage to property.

#### General notices

Contain **useful** information for users and instructions for avoiding malfunctions.

Signal word	Description
<b>Information:</b>	Useful information, application tips and instructions for avoiding malfunctions.

### 1.2.2 Introduction

The components of B&R's Secure Remote Maintenance solution have been designed, developed and manufactured for conventional use in industrial environments. They were not designed, developed and manufactured for any use involving serious risks or hazards that could lead to death, injury, serious physical impairment or loss of any kind without the implementation of exceptionally stringent safety precautions. In particular, these risks or dangers include the use of these devices to monitor nuclear reactions in nuclear power plants, from flight control or flight safety systems as well as in the control of mass transportation systems, medical life support systems or weapons systems.

All tasks such as the installation, commissioning and servicing of devices are only permitted to be carried out by qualified personnel. Qualified personnel are those familiar with the transport, mounting, installation, commissioning and operation of devices who also have the appropriate qualifications to perform these tasks (e.g. IEC 60364). National accident prevention regulations must be observed.

The safety notices, information about connection conditions (nameplate and documentation) and limit values specified in the technical data must be read carefully before installation and commissioning and are to be observed in all cases.

### 1.2.3 Intended use

Electronic devices are never completely failsafe. If the programmable logic controller, operating/monitoring device or uninterruptible power supply fails, the user is responsible for ensuring that other connected devices such as motors are brought to a safe state.

Modules from B&R are designed as "open equipment" (EN 61131-2) and "open type equipment" (UL). They are therefore designated for installation in an enclosed control cabinet. In all cases, it is necessary to observe and comply with all applicable national and international standards and guidelines, such as machinery directive 2006/42/EC.

### 1.2.4 Protection against electrostatic discharge

Electrical assemblies that can be damaged by **ElectroStatic Discharge** (ESD) must be handled accordingly.

#### 1.2.4.1 Packaging

- Electrical assemblies with housing  
... Do not require special ESD packaging but must be handled properly (see "[Electrical assemblies with housing](#)" on page 10).
- Electrical assemblies without housing  
... Are protected by ESD-suitable packaging.

### 1.2.4.2 Regulations for proper ESD handling

#### Electrical assemblies with housing

- Do not touch the male connector contacts on the device (bus data contacts).
- Do not touch the connector contacts of connected cables.
- Do not touch the contact tips on circuit boards

#### Electrical assemblies without housing

The following applies in addition to "Electrical assemblies with housing":

- All persons handling electrical assemblies and devices in which electrical assemblies are installed must be grounded.
- Assemblies are only permitted to be touched on the narrow sides or front plate.
- Always place assemblies on suitable surfaces (ESD packaging, conductive foam, etc.).

#### Information:

**Metallic surfaces are not suitable storage surfaces.**

- Assemblies must not be subjected to electrostatic discharges (e.g. due to charged plastics).
- A minimum distance of 10 cm from monitors or television sets must be maintained.
- Measuring instruments and devices must be grounded.
- Test probes of floating potential measuring instruments must be discharged briefly on suitable grounded surfaces before measurement.

#### Individual components

- ESD protective measures for individual components are implemented throughout B&R (conductive floors, shoes, wrist straps, etc.).
- The increased ESD protective measures for individual components are not required for handling B&R products at customer locations.

### 1.2.5 Transport and storage

During transport and storage, devices must be protected against undue stress (mechanical loads, temperature, moisture, corrosive atmospheres, etc.).

Devices contain components sensitive to electrostatic charges that can be damaged by improper handling. It is therefore necessary to provide the required protective measures against electrostatic discharge when installing or removing these devices (see ["Protection against electrostatic discharge" on page 9](#)).

### 1.2.6 Operation

#### 1.2.6.1 Protection against touching electrical parts

#### **Danger!**

**In order to operate programmable logic controllers, operating and monitoring devices and the uninterruptible power supply, it is necessary for certain components to carry dangerous voltages. Touching one of these components can result in a life-threatening electric shock. There is a risk of death, serious injury or damage to property.**

Before switching on the programmable logic controllers, operating and monitoring devices and uninterruptible power supply, it must be ensured that the housing is properly connected to ground potential (PE rail). The ground connection must also be made if the operating and monitoring device and uninterruptible power supply are only connected for testing purposes or only operated for a short time!

Before switching on the device, all voltage-carrying components must be securely covered. During operation, all covers must remain closed.

### 1.2.6.2 Ambient conditions - Dust, moisture, aggressive gases

The use of operating and monitoring devices (e.g. industrial PCs, Power Panels, Mobile Panels) and uninterruptible power supplies in dusty environments must be avoided. This can result in dust deposits that affect the functionality of the device. Sufficient cooling may then no longer be ensured, especially in systems with an active cooling unit (fan).

The presence of aggressive gases in the environment can also result in malfunctions. In combination with high temperature and relative humidity, aggressive gases – for example with sulfur, nitrogen and chlorine components – trigger chemical processes that can very quickly impair or damage electronic components. Blackened copper surfaces and cable ends in existing installations are indicators of aggressive gases.

When operated in rooms with dust and condensation that can endanger functionality, operating and monitoring devices such as Automation Panels or Power Panels are protected on the front against the ingress of dust and moisture when installed correctly (e.g. cutout installation). The back of all devices must be protected against the ingress of dust and moisture, however, or the dust deposits must be removed at suitable intervals.

### 1.2.6.3 Programs, viruses and malicious programs

Any data exchange or installation of software using data storage media (e.g. floppy disk, CD-ROM, USB flash drive) or via networks or the Internet poses a potential threat to the system. It is the direct responsibility of the user to avert these dangers and to take appropriate measures such as virus protection programs and firewalls to protect against them and to use only software from trustworthy sources.

## 1.2.7 Environmentally friendly disposal

All B&R control components are designed to inflict as little harm on the environment as possible.

### 1.2.7.1 Separation of materials

It is necessary to separate out the different materials so that devices can undergo an environmentally friendly recycling process.

Component	Disposal
Programmable logic controllers Operating/Monitoring devices Uninterruptible power supply Batteries and rechargeable batteries Cables	Electronics recycling
Cardboard/Paper packaging	Paper/Cardboard recycling
Plastic packaging material	Plastic recycling

Table 1: Separation of materials

Disposal must take place in accordance with applicable legal regulations.

## 2 Secure Remote Maintenance

---

B&R's Secure Remote Maintenance solution allows simple diagnostics and maintenance of machines and plants from a distance in accordance with current IT and security policies.

In addition, a certified and encrypted VPN connection is established between the SiteManager on the machine and a gateway, which is usually located at the machine manufacturer's service center. All access rights for up to 10000 machines can be stored there. The SiteManager has integrated digital inputs and outputs. These can be used to connect a key switch, for example, that must be actuated to permit access for maintenance. An integrated firewall provides protection against unauthorized third-party access. In order to avoid security conflicts with plant firewalls, communication with the Internet is handled using firewall-compatible encrypted Web protocols. Therefore, no additional ports must be opened.

### **Warning!**

**Local personnel must be informed whenever access takes place. The user must implement suitable measures to ensure that remote access is not possible without notifying local personnel.**

### **Machine pool management**

Machine builders have many customers – and even more machines in the field. In order to use remote maintenance effectively, centralized machine pool management is a must-have subsystem of a modern remote maintenance solution. This manages the machines in the field as well as the access rights of service staff operating the individual machines. A machine pool management system is the most important function of an easy-to-use, Secure Remote Maintenance system. Access to machine pool management is possible via a web portal that is accessible via the Internet. This web portal is part of the GateManager.

### **Possibilities**

- Diagnostics using the System Diagnostics Manager in Automation Studio
- Read logbook entries and application data
- Change machine settings and parameters
- Updating programs and firmware via Automation Studio



## Strong partnership with technology leader

The Secure Remote Maintenance solution is a brand labeled product that is developed by Secomea. Secomea is a leading manufacturer of industrial communication equipment with a strong focus on security and usability of the products.

The B&R versions of the hardware and software products used are slightly different than the Secomea products:

- All B&R SiteManagers are fully integrated in Automation Studio and can therefore be configured in the Automation Studio project.

### **Information:**

**The Secomea SiteManagers cannot be configured that way.**

- In addition, B&R versions of the GateManager, SiteManager and LinkManager software variants are used.

### **Information:**

**The software versions from Secomea are not compatible with the B&R versions and are not permitted to be used with B&R's Secure Remote Maintenance solution!**

- For a LinkManager connection via VNC protocol, a dedicated VNC agent must be used (dedicated entry of address and port number, e.g. 192.168.0.8:5910).

### **Information:**

**With the Secomea solution, VNC port 5900 is always used by default.**

- Only GateManager Premium Administrator accounts are used at B&R.

### 3 System overview

B&R's Secure Remote Maintenance solution was developed to provide the highest level of network security as well as simple and intuitive operation in order to give a service technician remote access to a machine. For this purpose, a secure connection is established between the machine and the service technician during a service call. The service technician only needs a web browser and an Internet connection in order to log onto the GateManager web portal. The machine also connects to the web portal via the SiteManager, a remote maintenance gateway with built-in firewall. The Machine Pool Manager integrated in the web portal then allows authorized connections to be made between the service technician and the machine, and a secure VPN connection is established.

VPN networks, firewalls and appropriate strategies for establishing a connection provide maximum protection for the remote connection. This protection even extends to man-in-the-middle and denial-of-service attacks and makes the remote maintenance solution as secure as possible.

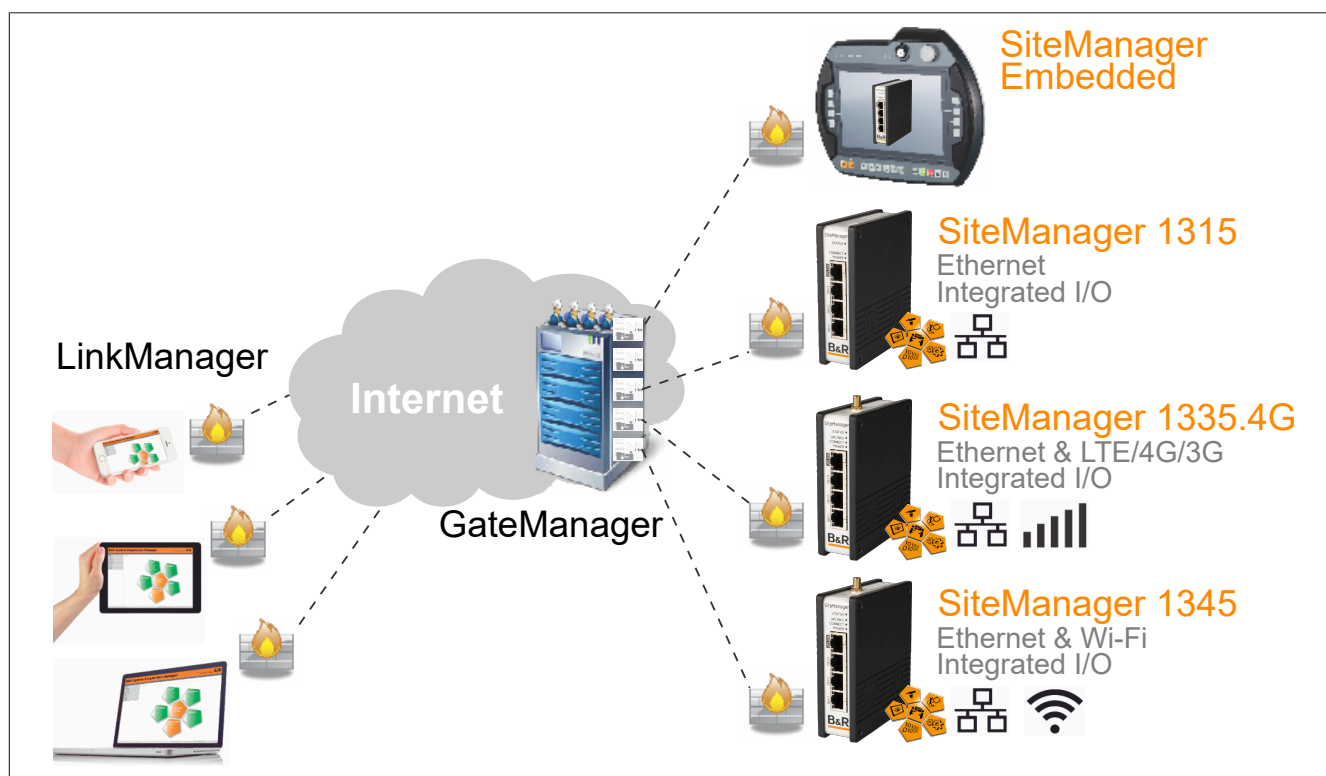
In cases where a LAN or WLAN connection is not possible or not desired, the VPN connection can be established via a mobile network.

#### System design

Secure Remote Maintenance consists of at least the following components:

- 1x GateManager ("B&R hosting service" included in the "Starter" package or 0RMGM.sw)
- 1x LinkManager (0RMLM.WIN) and LinkManager Mobile (0RMLM.MOB) license
- 1x SiteManager (0RSM13x5) or SiteManager Embedded (0RSMSE.x)
- Service agreement

Based on this minimum configuration, various starter packages are offered for quick entry into the remote maintenance solution (see ["Starter package" on page 42](#)).



## 3.1 GateManager

The GateManager is the central connection platform for technicians and machines, which both dial in to establish a connection (the GateManager acts as a secure proxy for the SiteManager and LinkManager). Connections are established according to the defined authorization settings i.e. the configured user accounts and access rights. User accounts, authorization settings and machines can be managed easily and intuitively by authorized personnel via a web portal (Machine Pool Management).

The GateManager is offered by B&R as a hosting service and software installer (Linux) and can be set up according to specific customer requirements. This allows the machine builder to set up a customized portal to gain an overview of machines in the field.

The GateManager is the only component that has open ports to the Internet. This means that the GateManager must be equipped with a fully qualified domain name (FQDN); its user interface is also web-based, of course. In these respects, the GateManager is no different from a normal web server on which the company website is hosted, for example. Access and connections are only permitted with the correct X.509 certificate.

Administrators of an own instance (software image) have the possibility to create "domains". Domains are used to structure and subdivide a GateManager in a logical manner. Each domain can be assigned one more domain administrators that can only view and manage the content of the assigned domain.

### Information:

**GateManagers are delivered with a LinkManager and LinkManager Mobile license preinstalled.**

#### Software installer for Linux

The GateManager software variant is based on a software installer for any Linux environments. Download the GateManager software via <http://www.br-automation.com/gatemanager>.

#### GateManager hosting service

Various starter packages (see "[Starter package](#)" on page 42), which include the GateManager hosting service, are offered for quick entry into the remote maintenance solution.

With the GateManager hosting service, the Secure Remote Maintenance solution can be used without having to install and operate a GateManager. This relieves the customer the initial expenses for purchasing the GateManager variant and does away with the need for integration in their IT landscape.

#### Email sizes

In Secomea's hosting service, emails can be sent with a maximum size of 10 MB, including the header. This corresponds to an email size of about 7 to 8 MB.

#### 3.1.1 Order data

Order number	Short description
	<b>GateManager</b>
0RMGM.SW	Secure Remote Maintenance - GateManager (software version), manages max. 10000 SiteManagers, 1x LinkManager and 1x LinkManager Mobile license included, service fee 0RMAS.SERVICE-01 must be paid separately.

Table 2: 0RMGM.SW - Order data

### Information:

**Download the GateManager software via <http://www.br-automation.com/gatemanager>.**

### 3.1.2 Activating the GateManager

A GateManager is delivered in trial/demo mode. There is 1 LinkManager and 1 LinkManager Mobile license pre-installed; a maximum of 3 SiteManagers and 2 at the same time can be managed. There are no functional restrictions in demo mode.

To use the GateManager to its full extent, it must be activated. For activation, the license ID and hostname of the GateManager must be reported to B&R. Based on this information, a license key is generated that can be used to activate the GateManager (a license is created only for a particular GateManager identified by its license ID and hostname). LinkManager and LinkManager Mobile licenses and users are all managed in the GateManager.

#### Information:

The hostname can be freely defined in the GateManager settings and must be an FQDN, e.g. "remote.companyname.com". The use of an IP address instead of an FQDN is not supported for generating licenses. In addition, please note that changes are not permitted to be made after the hostname has been successfully activated since this would invalidate all installed licenses.

The GateManager includes a special form to simplify the process of transferring the GateManager information to a B&R representative.

The screenshot shows the 'License Ordering Specification' form. At the top, there are tabs for 'Tree', 'Files', 'Licenses', and 'Server'. Below these are sub-tabs for 'Status', 'Shortage', 'Install', and 'Order'. The form contains the following sections:

- Section 1: Your local B&R representative:** Includes input fields for 'Company:', 'Contact:', and 'E-mail:'.
- Section 2: Order Reference:** Displays pre-filled information: 'GateManager Model: 4260', 'Hostname (FQDN): remote.testcompany.com', and 'LicenseID: 1234567890abCdeFGHIjklm'. It also has input fields for 'Order number:', 'Your company:', 'Your name:' (pre-filled with 'Max Mustermann'), 'Your E-mail:' (pre-filled with 'max.mustermann@testcompany.com'), and a 'Comment:' field.
- Section 3: Current Agreement of Service and Licenses:** Shows the current status: 'Current Agreement of Service: Trial mode', 'LinkManager Licenses: 1 of 1 installed', 'LinkManager Mobile Licenses: 1 of 1 installed', and 'SiteManagers: 1 of 3 added'.

A 'Submit Information' button is located at the bottom left of the form.

The form must be filled in as follows:

1. Specify the B&R representative information. This is included on the delivery note of the GateManager, for example. Please use the contact and email field to enter the name and email address of the B&R sales representative or a B&R subsidiary.
2. The required GateManager information is entered automatically. Please enter here the order number from the GateManager delivery note and the name of the company. Additional information can be specified via the comment field.
3. This section shows the currently active service agreement for the GateManager. It also shows how many licenses and SiteManagers are installed and how they can be added to this service agreement.

By clicking **<Submit Information>**, the complete form is sent to B&R and to the B&R representative.

### 3.1.2.1 Delivery and installation of licenses

B&R then compares the transferred data with the existing order data. After successful verification, the activation license is automatically transferred to and installed on the GateManager to be activated. Since licenses are tied to "hostname" and "license-id" of the GateManager, there is no need to archive the licensing files. For this reason, licenses are delivered during the automatic installation process on the GateManager.

If the GateManager is offline or otherwise unreachable, delivery takes place via email to the email address specified under item 2 on the form. The email also contains instructions for installing the licenses.

The delivery and installation procedure is identical for the activation license and all other GateManager licenses (LinkManager / LinkManager Mobile licenses, SiteManager Embedded licenses, etc.). Licenses are delivered exclusively in digital form.

### 3.1.3 Service fee

The remote maintenance solution is subject to a service agreement with a corresponding service fee. The service fee includes software updates, security patches, maintenance, B&R support and hosting service.

#### Information:

**The service fee must be paid in advance. The remote maintenance solution can be used at no cost for the first 12 months.**

#### 3.1.3.1 Order data

Order number	Short description
ORMAS.SERVICE-01	Secure Remote Maintenance - Service fee per year - includes software updates and patches as well as bug fixes, first 12 months at no cost, billing in advance

### 3.1.4 Additional services

#### 3.1.4.1 LogTunnel - Remote data logging

LogTunnel makes it possible to record machine data to a central database server (log server) in the machine manufacturer's data center.

##### 3.1.4.1.1 Order data

Order number	Short description
ORMAS.LOG	Secure Remote Maintenance - Activation of LogTunnel and usage statistics license

#### 3.1.4.2 SMS license

##### 3.1.4.2.1 Order data

Order number	Short description
ORMAS.SMS	Remote Maintenance - Activation of SMS license

### 3.1.5 User authorization management

All user accounts on the remote maintenance system are set up and serviced on the GateManager. Each user account must be assigned a user role that allows certain activities in the remote maintenance system. This user authorization management acts as function separation and represents another important data link layer in the remote maintenance system.

The GateManager logs, among other things, every change in the configuration, every user login, every connection established with a user account, executed actions and events. All these events are logged with a timestamp, description and the user who executed them.

The most important user roles are:

- GateManager server administrator
- GateManager domain administrator
- LinkManager user
- LinkManager Mobile users
- Domain observer

The system can be configured in such a way that access to the SiteManager and its device agents are only carried out by LinkManager users. Administrators then cannot establish any connections to SiteManagers or device agents within the GateManager user interface. Administrators can then only assign the SiteManager and LinkManager user accounts to domains or subdomains.

#### 3.1.5.1 GateManager server administrator

The user role is used for a system administrator. The server administrator's task is to create the initial server configuration and to ensure continued error-free operation. The server administrator can set up, approve, disable, etc. all available user roles for users.

The server administrator has access to all domains on the GateManager. The most important tasks that can be performed with a server administrator user account are listed below:

- Creating additional server administrator user accounts and user accounts with other roles
- Access to the GateManager configuration (email settings, server log, license maintenance, firmware repository, etc.)
- Creating backups of SiteManager settings
- Upgrading SiteManager firmware
- Creating actions and alerts
- Creating domains and subdomains
- Moving user accounts, SiteManagers and device agents throughout domains.

#### 3.1.5.2 GateManager domain administrator

This user role is similar to the one for a server administrator. The domain administrator can set up and maintain user accounts in their assigned domain as well as create subdomains and subdivide their domain in this way. The domain administrator has no information about possible additional domains that are still located on the GateManager. The domain administrator can also arrange SiteManagers and device agents into subdomains and in this way allow or deny LinkManagers user accounts access to machines.

Activities are listed below that can be carried out with a domain administrator user account. This is only possible in the domain which the domain administrator is responsible for:

- Creating user accounts (no server administrator users!)
- Creating backups of SiteManager settings
- Upgrading SiteManager firmware
- Creating actions and alerts
- Creating subdomains
- Moving user accounts, SiteManagers and device agents into subdomains.

### 3.1.5.3 LinkManager user

This user role is intended for a service technician who requires access to machines or machine components. Via pre-configured device agents, the service technician can connect via PC to the device agents. LinkManager users are dependent on the correct configuration of their access rights to SiteManager and their device agents by the domain administrator.

### 3.1.5.4 LinkManager Mobile users

LinkManager Mobile allows users remote access to industrial equipment from their iPhone, iPad or Android device. The app is designed to access graphical user interfaces such as PLC devices, HMI control panels or webcams. It also connects to desktops running Linux or Windows. LinkManager Mobile can be used to easily connect with the device, start a VNC or MS Remote Desktop (RDP) client and then control the device remotely.

### 3.1.5.5 Domain observer

This user role provides the user insight into all details of a domain, including audit logs, licenses as well as SiteManagers and device agents. This role is only for monitoring and viewing activities in a domain. The domain observer can neither make changes to the configuration nor set up new user accounts.

## 3.2 SiteManager

**SiteManagers** 0RMSM1315, 0RMSM1335.4G and 0RMSM1345 allow the machine or machine network to connect to the GateManager and further to the Internet. All SiteManager variants are equipped with integrated inputs and outputs as well as at least one Ethernet interface for the uplink to the Internet. The integrated firewall controls all access to the machine network. This means that communication between the GateManager and machine network is not possible if corresponding firewall rules have not been created (version 8.2 and later).

All SiteManager variants can be configured in Automation Studio. The SiteManager must only be installed once. If it becomes necessary to replace the SiteManager, all parameters are transferred from the machine's PLC controller to the new SiteManager. When the SiteManager logs onto the Service Portal for the first time, one-time authentication is all that is necessary.

### SiteManager Embedded

SiteManager Embedded is the software variant for the SiteManager and can be used on x86 Windows and Linux Automation/Panel PCs. SiteManager Embedded for LinkManager offers the same access possibilities to the machine network as the hardware variants of the SiteManager.

Simply download and install the SiteManager Embedded installation package. Download the SiteManager software via <http://www.br-automation.com/sitemanager>.

SiteManager Embedded licenses are installed on the GateManager and assigned to SiteManager Embedded instances.

SiteManager Embedded is available in 2 variants:

- **SiteManager Embedded BASIC:** The BASIC variant allows access on the Automation/Panel PC where SiteManager Embedded is installed. It is not possible to use hypervisor functionality in this variant, however. Accessing the machine network and network stations contained therein is not possible.
- **SiteManager Embedded EXTENDED:** The EXTENDED variant is based on the functionality of the BASIC variant and additionally permits access to the machine network and other network stations as well as the use of hypervisor functionality of Automation/Panel PCs. This variant offers the same range of functions as the hardware SiteManager.

### SiteManager hardware

The SiteManager hardware variants are primarily distinguished by the number of uplink ports available:

- **SiteManager 1315:** 1x Ethernet uplink port
- **SiteManager 1335.4G:** 1x LTE/4G/3G uplink port and 1x Ethernet uplink port
- **SiteManager 1345:** 1x Wi-Fi uplink port and 1x Ethernet uplink port

### 3.2.1 Model comparison

SiteManager model comparison	0RMSM11xx	0RMSM13xx	SiteManager Embedded BASIC	SiteManager Embedded EXTENDED
Remote access to IP devices (UDP/TCP)	Yes	Yes	Yes	Yes
Remote access to USB / serial / layer 2 devices	Yes	Yes	No	No
Tunnel access to the ENTIRE remote network	Yes	Yes	Yes	Yes
Number of individual device agents	Up to 5	Up to 10	2	Up to 5
Access gateway for other IP devices	Yes	Yes	No	Yes
Data collection module (DCM)	Yes	Yes	No	Yes <sup>1)</sup>
Configurable forwarding/routing rules	Yes	Yes	No	No
Automatic detection of Ethernet and USB devices	Yes	Yes	No	No
LogTunnel clients support	Yes	Yes	No	Yes
LogTunnel master push support	Yes	Yes	No	Yes
LogTunnel master pull support	Yes	Yes	No	Yes <sup>1)</sup>

1) Only available for Linux



### 3.2.2 Order data

#### 3.2.2.1 SiteManager Embedded

##### 0RMSME.x

Model number	Short description
	<b>SiteManager</b>
0RMSME.B	Secure Remote Maintenance - SiteManager embedded BASIC license for Windows/Linux, 2 device agents
0RMSME.E	Secure Remote Maintenance - SiteManager embedded EXTENDED license for Windows/Linux, 5 device agents

Table 3: 0RMSME.B, 0RMSME.E - Order data

## Information:

Download the SiteManager software via <http://www.br-automation.com/sitemanager>.

#### 3.2.2.2 SiteManager hardware

##### 0RMSM1315


Order number	Short description	Figure
	<b>SiteManager</b>	
0RMSM1315	Secure Remote Maintenance -SiteManager, LAN 1x Ethernet 100BASE-T uplink connection, 3x device connections, 10 device agents, integrated firewall, 2x digital inputs, 2x digital outputs, 24 VDC	
	<b>Optional accessories</b>	
	<b>Terminal blocks</b>	
0TB6110.2010-01	Accessory terminal block, 10-pin (3.81), screw clamp terminal block 1.5 mm <sup>2</sup>	

Table 4: 0RMSM1315 - Order data

##### 0RMSM1335.4G


Order number	Short description	Figure
	<b>SiteManager</b>	
0RMSM1335.4G	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T uplink connection, 1x GPRS/3G/4G uplink connection, 3x device connections, 10 device agents, integrated firewall, 2x digital inputs, 2x digital outputs, 24 VDC	
	<b>Optional accessories</b>	
	<b>Antennas</b>	
0RMSM.A3G-10	GSM/3G puck antenna Frequencies: 880-960/1710-2170 MHz, SMA connector (male), 2.5 m cable, Screw or hole mounting, IP67, compatible with 0RMSM1x35	
0RMSM.A3G-20	GSM/3G mini antenna Frequencies: 824-960/1710-2170 MHz, SMA connector (male), 3 m cable, magnetic attachment, compatible with 0RMSM1x35	
0RMSM.AMB-10	GSM/3G/LTE broadband antenna Frequencies: 750-1250, 1650-2700 MHz, male SMA connector, 3 m cable, screw and hole installation, compatible with 0RMSM1x35, base plate needed for optimal amplification, IP67	
	<b>Terminal blocks</b>	
0TB6110.2010-01	Accessory terminal block, 10-pin (3.81), screw clamp terminal block 1.5 mm <sup>2</sup>	

Table 5: 0RMSM1335.4G - Order data

**0RMSM1345**


Order number	Short description	Figure
	<b>SiteManager</b>	
0RMSM1345	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T uplink connection, 1x Wi-Fi uplink connection, 3x device connections, 10 device agents, integrated firewall, 2x digital inputs, 2x digital outputs, 24 VDC	
	<b>Optional accessories</b>	
	<b>Antennas</b>	
0RMSM.AWIFI-10	Wi-Fi puck antenna, 2.4 & 5 GHz, compatible with 0RMSM1x45, 2 m cable	
	<b>Terminal blocks</b>	
0TB6110.2010-01	Accessory terminal block, 10-pin (3.81), screw clamp terminal block 1.5 mm <sup>2</sup>	

Table 6: 0RMSM1345 - Order data

**Content of delivery:**

Quantity	Description
1	Wi-Fi antenna, 2.4 GHz, compatible with 0RMSM1345, swivel option with RP-SMA connector

### 3.2.3 Technical data

#### 3.2.3.1 SiteManager Embedded

Order number	0RMSME.B	0RMSME.E
<b>General information</b>		
System requirements		
Hardware requirements		
Processor	Intel x86 or compatible CPU	
RAM	10 MB of free RAM	
Hard drive space	5 MB	
Software requirements		
Operating system	Windows: 7/8/10, 32/64-bit, standard or embedded Linux: Typical x86 distributions: Debian, Ubuntu, CentOS, etc.	

#### 3.2.3.2 SiteManager hardware (0RMSM13x5)

Product ID	0RMSM1315	0RMSM1335.4G	0RMSM1345
General information			
B&R ID code	0x6C5E	0x6C5F	0x6C60
Reset button	Yes		
Status LED	Supply voltage Status LinkManager connection	Supply voltage Status LinkManager connection Wireless connection	
Power consumption	Max. 5 W (without USB) Max. 8 W (with USB)		
Functionality			
Data transfer / Frequency domain			
Integrated broadband modem			
LTE band	-	See 0RMSM1335.4G bands.	-
WCDMA/UMTS	-	See 0RMSM1335.4G bands.	-
GPRS/EDGE	-	B2 (1900) B3 (1800) B5 (850) B8 (900)	-
Integrated Wi-Fi module	-		2.4 GHz 5 GHz
Controller			
Processor			
Type	ARM Cortex-A7 MCU		
Clock frequency	800 MHz		
Interfaces			
RS232	DB9 serial interface with full data flow control		
USB			
Quantity	1		
Type	USB 2.0		
Interface IF1			
Type	Ethernet UPLINK1		
Variant	Shielded RJ45		
Line length	Max. 100 m between 2 nodes (segment length)		
Transfer rate	Max. 10/100 Mbit/s		
Transfer			
Physical layer	10BASE-T/100BASE-TX		
Half-duplex	Yes		
Full-duplex	Yes		
Autonegotiation	Yes		
Auto-MDI/MDIX	Yes		
Interface IF2			
Type	DEV1		
Variant	Shielded RJ45		
Transfer rate	Max. 10/100 Mbit/s		
Interface IF3			
Type	-	4G/3G/GPRS	-
Variant	-	SMA female	-
Transfer rate	-	Downlink: 50 Mbit/s (10 MHz bandwidth) Uplink: 25 Mbit/s (10 MHz bandwidth)	-
Interface IF4			
Type	-		Wi-Fi
Variant	-		RP-SMA female
Interface IF5			
Type	DEV2		
Variant	Shielded RJ45		
Transfer rate	Max. 10/100 Mbit/s		

## System overview

Product ID	0RMSM1315	0RMSM1335.4G	0RMSM1345
Interface IF6			
Type		DEV3	
Variant		Shielded RJ45	
Transfer rate		Max. 10/100 Mbit/s	
<b>Electrical properties</b>			
Nominal voltage		12 to 24 VDC	
<b>Operating conditions</b>			
Degree of protection per EN 60529		IP20	
<b>Ambient conditions</b>			
Temperature			
Operation		-25 to 60°C	
Storage		-40 to 60°C	
Relative humidity			
Operation		5 to 95%	
Storage		5 to 95%	
Transport		5 to 95%	
Elevation			
Operation		2000 m	
<b>Mechanical properties</b>			
Material		Aluminum	
Dimensions			
Width		32 mm	
Height		107 mm	
Depth		97 mm	
Weight		0.5 kg	

## 0RMSM1335.4G bands

	LTE bands	WCDMA/UMTS bands
B1 (FDD 2100) IMT	X	X
B2 (FDD 1900) PCS	X	X
B3 (1800 +) DCS	X	
B4 (1700) AWS	X	X
B5 (850) CLR, US, Korea, etc.	X	X
B6 (850) Japan #1		X
B7 (2600) IMT-E	X	
B8 (900) E-GSM	X	X
B12 (700) US	X	
B13 (700c) USMH, LSMH US	X	
B18 (800 or 850?) Japan #4	X	
B19 (800 or 850?) Japan #5	X	X
B20 (800) digital dividend	X	
B25 (1900 b Block)	X	
B26 (850+) extended CLR	X	
B28 (700 APT) APAC	X	
B34 (TDD)	X	
B38 (TDD 2600) IMT-E	X	
B39 (TDD 1900 +) China	X	
B40 (TDD 2300) China	X	
B41 (TDD 2500) BRS/EBS	X	
B66 (TDD)	X	

### 3.2.4 Accessories

#### 3.2.4.1 Terminal blocks

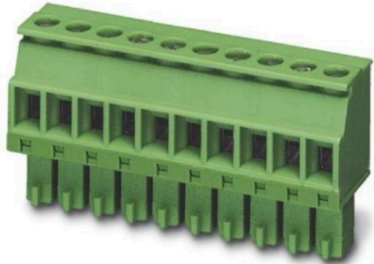
Order number	Short description	Figure
	<b>Terminal blocks</b>	
0TB6110.2010-01	Accessory terminal block, 10-pin (3.81), screw clamp terminal block 1.5 mm <sup>2</sup>	

Table 7: 0TB6110.2010-01 - Order data

#### 3.2.4.2 Antennas

##### Information:

**When installing the SiteManager in the control cabinet and using an antenna, mounting the antenna outside the control cabinet is recommended!**

**For UL conformity, the antenna must be mounted outside the control cabinet!**


Order number	Short description	Figure
	<b>Antennas</b>	
0RMSM.A3G-10	GSM/3G puck antenna Frequencies: 880-960/1710-2170 MHz, SMA connector (male), 2.5 m cable, Screw or hole mounting, IP67, compatible with 0RMSM1x35	

Table 8: 0RMSM.A3G-10 - Order data


Order number	Short description	Figure
	<b>Antennas</b>	
0RMSM.A3G-20	GSM/3G mini antenna Frequencies: 824-960/1710-2170 MHz, SMA connector (male), 3 m cable, magnetic attachment, compatible with 0RMSM1x35	

Table 9: 0RMSM.A3G-20 - Order data


Order number	Short description	Figure
0RMSM.AMB-10	<b>Antennas</b>	
	GSM/3G/LTE broadband antenna Frequencies: 750-1250, 1650-2700 MHz, male SMA connector, 3 m cable, screw and hole installation, compatible with 0RMSM1x35, base plate needed for optimal amplification, IP67	

Table 10: 0RMSM.AMB-10 - Order data


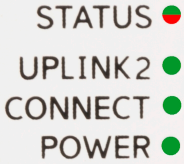
Order number	Short description	Figure
0RMSM.AWIFI-10	<b>Antennas</b>	
	Wi-Fi puck antenna, 2.4 & 5 GHz, compatible with 0RMSM1x45, 2 m cable	

Table 11: 0RMSM.AWIFI-10 - Order data

### 3.2.5 LED status indicators

All variants have 3 LEDs to indicate the module power supply, module status and LinkManager connection. For variants 1x35 and 1x45, another LED is available that is used to indicate the status of the wireless connection:

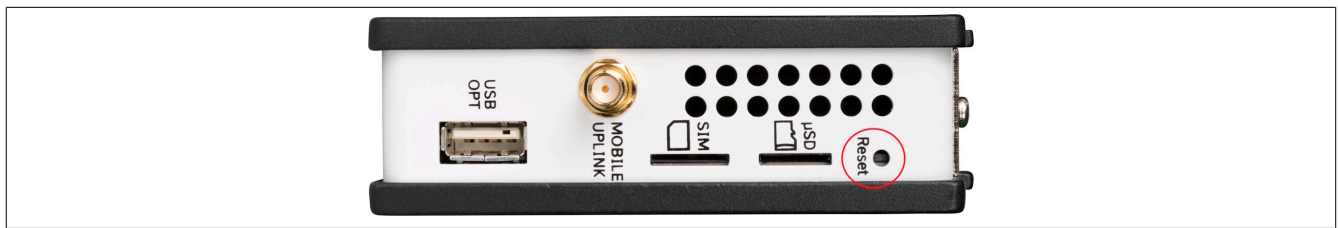
Figure	LED	Color	Status	Description
	STATUS	Red	Continuous blinking	Booting
			Blinks 2x	GateManager disconnected or in the process of establishing a connection.
			On	Possible causes: <ul style="list-style-type: none"> <li>• UPLINK is physically disconnected.</li> <li>• GateManager configuration is missing on the SiteManager.</li> <li>• No connection to the GateManager host because its address is configured as DNS name and a DNS server has not been configured or is not accessible or is not functioning properly.</li> </ul>
	UPLINK2	Green	On	GateManager connected.
		Green	Off	<b>1x35:</b> No SIM card detected.
				<b>1x45:</b> Possible causes: <ul style="list-style-type: none"> <li>• No Wi-Fi SSID configured.</li> <li>• SSID configured, but no Wi-Fi key configured.</li> <li>• SSID and Wi-Fi key configured, but no access point that matches the SSID found.</li> </ul>
				<b>1x35:</b> Incorrect or missing SIM PIN code.
				<b>1x35:</b> SIM PIN code OK, but no connection (error correction in the SiteManager user interface).
				<b>1x45:</b> Wi-Fi SSID found, but not yet connected. Possible error with Wi-Fi key.
				<b>1x35:</b> Connection successful. Slow connection (GPRS).
				<b>1x35:</b> Connection successful. Fast connection.
				<b>1x45:</b> Wi-Fi connected successfully.
	CONNECT	Green	Long pause + Blinks 2x	Remote management is disabled using <b>input 1</b> or the SiteManager user interface.
			On	LinkManager connected.
	POWER	Green	On	Power supplied.

#### Information:

It is important to note that it may take some time until the LED status indicator indicates a new status. For example, it may – depending on the keep alive interval setting on the GateManager – take up to 4 minutes until the disconnecting the GateManager is indicated.

### 3.2.6 Operating and connection elements

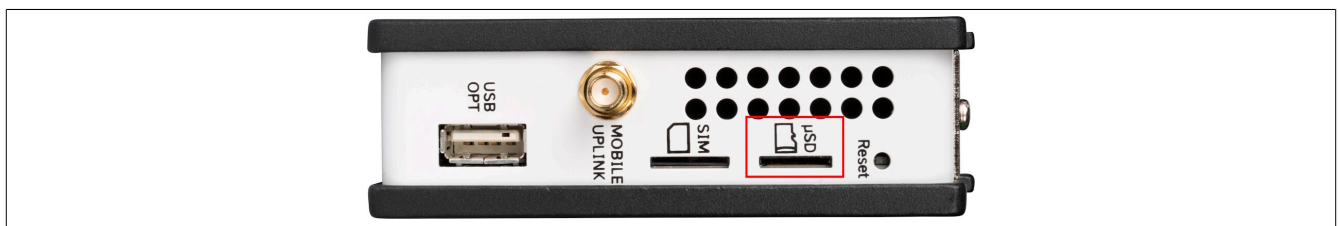
#### 3.2.6.1 Reset button



The SiteManager has a reset button on the top that can also be used to restore the factory settings.

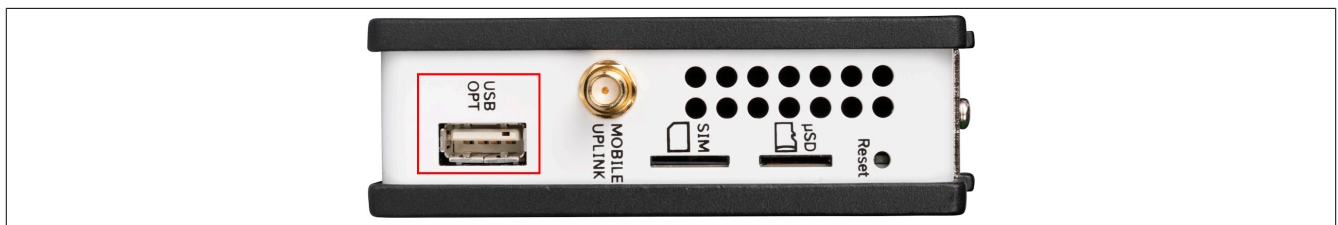
- If the reset button is pressed, the SiteManager is restarted.
- If the reset button is pressed for more than 5 seconds, the SiteManager is not only restarted but also reset to the factory settings.

#### 3.2.6.2 SD card slot



The SiteManager is equipped with a microSD slot on the top side. This makes it possible to expand the internal memory of the SiteManager using a SD memory card. This memory expansion can only be used for the data collection module (DCM), however.

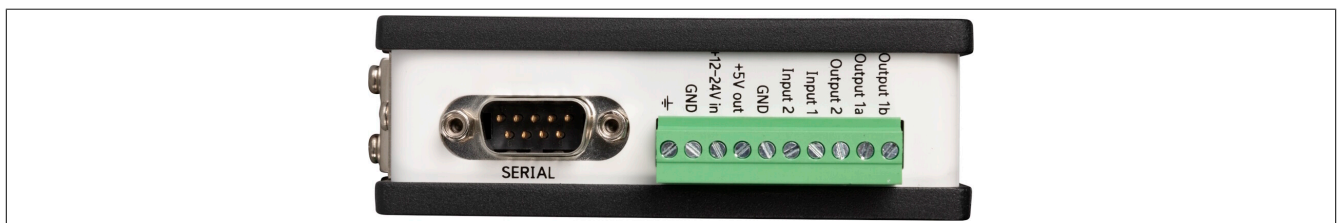
#### 3.2.6.3 USB interface



The SiteManager is equipped with a USB interface on the top side. This can be used for the following options, for example:

- For initial setup (see ["Using a USB flash drive" on page 33](#))
- Use as storage medium (max. 2 GB)
- Use for USB Wi-Fi adapter (see [Wi-Fi USB adapter with SMA initial contact](#))

#### 3.2.6.4 Serial interface



The SiteManager is equipped with a serial interface on the underside. The serial interface offers the option of connecting to devices that do not yet have an Ethernet interface (e.g. old controllers in existing systems).

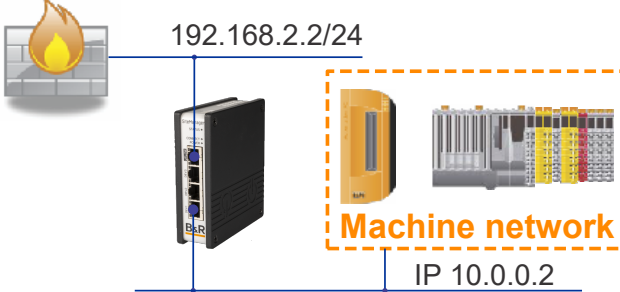
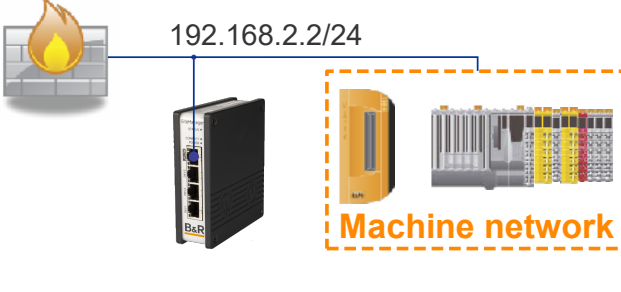
### 3.2.6.5 Ethernet interfaces (DEV1/2/3 and UPLINK1)

The SiteManager is equipped with Ethernet interfaces on the front. A standard Ethernet patch cable (straight or crossover) must be used to connect the UPLINK1 interface to a switch on a network with Internet access.

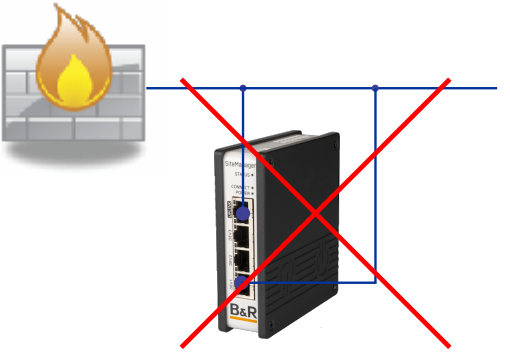
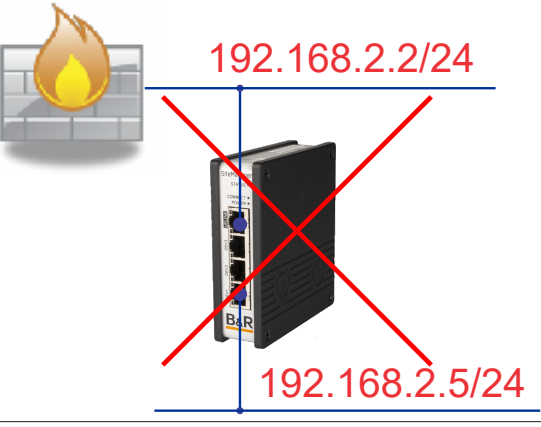
#### Default settings

DEV1 to DEV3 are configured as switches; the settings of the DEV1 port are applied to DEV2 and DEV3. DEV2 and DEV3 can also be separated; the settings must be made directly on the SiteManager via the user interface for this. This requires additional expert knowledge in the field of network technology, however. Using this feature is therefore only recommended in exceptional cases.

See the following options for cabling and configurations:

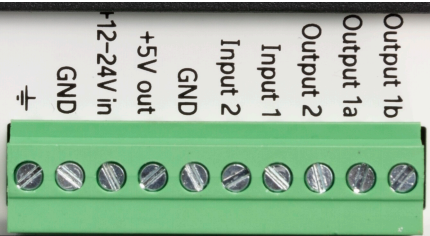
 <p>The DEVx port can be connected to an existing network that is separate from the UPLINK1 network, or a separate device network can be created isolated from the UPLINK1 network.</p>	 <p>It is also possible to only connect the UPLINK1 interface and only make devices accessible on the uplink side.</p>
--	--

The following are some forbidden cabling and configuration scenarios.

 <p>Do not connect the DEVx and UPLINK1 ports to the same physical network.</p>	 <p>Do not assign the DEVx address in the same logical network as UPLINK1.</p>
---	---

### 3.2.6.6 Power supply

The SiteManager has connectors on the bottom. The power supply is only permitted to be applied to the **GND** and **+12 to 24 V In** connections!


--

#### Information:

It is recommended to connect the grounding to reduce noise.



### 3.2.6.7 I/O interfaces

SiteManager has connectors on the bottom side.



#### Digital inputs (Input 1, Input 2):

The digital inputs are in state "OFF" (inactive) at 2.34 V or higher and in state "ON" at 0.16 V or lower. The behavior for input voltages between 0.16 V and 2.34 V is undefined. There is an internal 10 kΩ pull-up resistor at 3.3 V so that an unconnected input is in state "OFF".

**Input 1** is intended by default to toggle GateManager access. This makes it possible to connect a simple on/off switch to control when remote maintenance should be permitted.

Configurable **Input 2** can be used for user-defined email / SMS text message alarms.

#### Relay output (Output 1a and Output 1b):

**Output 1** is a "dual-pin" connector on which both pins are isolated in the "OFF" state and shorted together in the "ON" state. The maximum sink current is 0.5 A and the maximum voltage is 24 V.

By default, the output is configured so that it is active if a LinkManager is connected and can be used to turn on a lamp that informs the user that the device is being used.

#### Digital output (Output 2)

**Output 2** is a "single-pin" connector that is connected to GND in state "ON" and has high resistance state "OFF". The connection is of type "Open drain", i.e. (as with a switch) no voltage is output at the connection itself, but must be supplied either from an external source (max. 24 V) or from connection **+5 V out**. In state "OFF" (inactive), the impedance is at least 24 MΩ. In state "ON", the impedance is max. 0.5 Ω. The maximum sink current is 0.2 A.

#### 3.2.6.7.1 Wiring the inputs/outputs

For a general description of how to use SiteManager inputs and outputs, see [SiteManager xx29, xx39 and xx49 - Working with I/O Ports](#), or consult the online help installed on the SiteManager (select menu option **HELP**).

#### Notice!

To ensure error-free operation, it is strongly recommended to connect the inputs and outputs using a relay circuit. With respect to the individual I/O channels:

- Output 1: Floating
- Output 2: B&R input module (sink) (e.g. X20DI2372)
- Input 1: B&R relay module (e.g. X20DO4649)
- Input 2: B&R relay module (e.g. X20DO4649)

#### Notice!

Do not connect voltages (e.g. 24 V) directly to a SiteManager output. This could permanently damage the output connection.

#### Information:

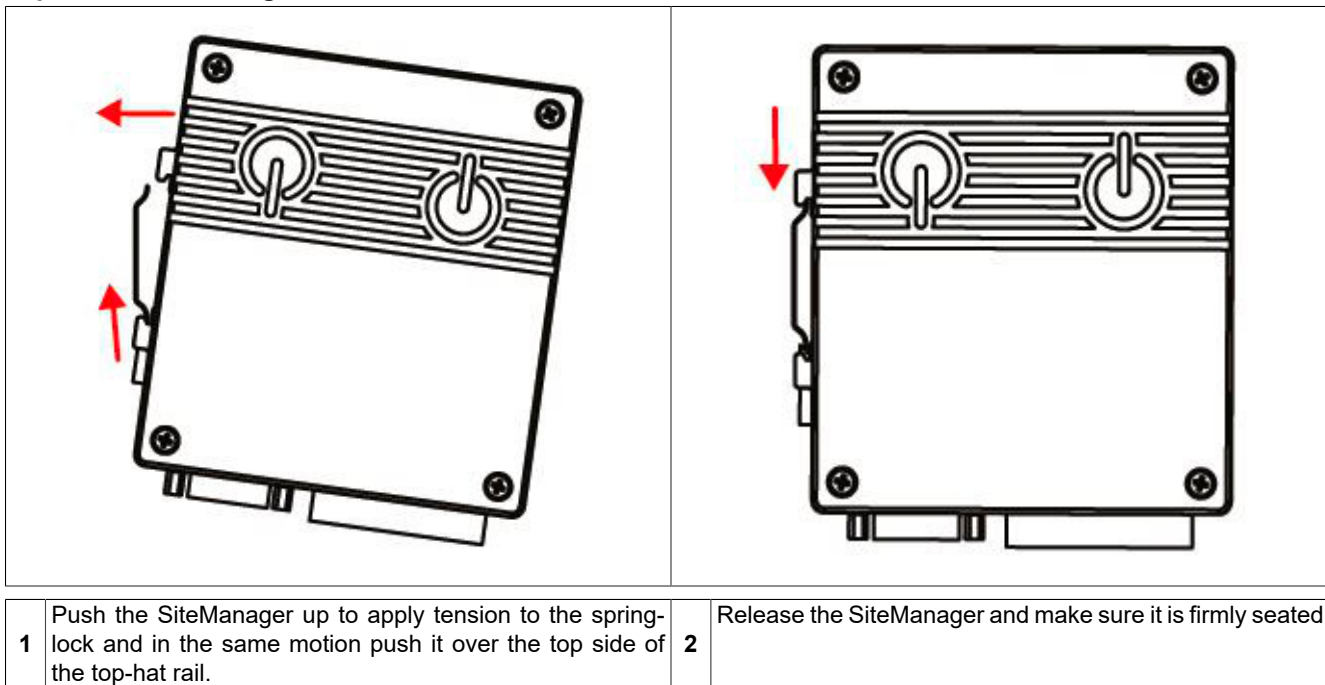
In addition to the power supply, the SiteManager also has a GND and a permanent 5 V output. It is recommended to use these to connect the SiteManager's inputs and outputs.

### 3.2.7 Installation

A top-hat rail conforming to the EN 60715 standard (TH35-7.5) is required to mount a SiteManager.

For optimal cooling and air circulation, there must be at least 35 mm free space above the modules. There must be at least 10 mm of free space on the left and right sides. Underneath the modules, 35 mm space must be left free for I/O and power supply cabling.

#### Top-hat rail mounting



#### Information:

**When installing the SiteManager in the control cabinet and using an antenna, mounting the antenna outside the control cabinet is recommended!**

#### Conditions for UL-compliant mounting

For a UL-compliant mounting, the following points must be taken into account:

- The SiteManager must be supplied using a SELV/PELV source. In addition, a max. 3 A fuse per UL CCN JDYX2/8 must be used.
- An antenna must be installed outside the control cabinet. Suitable cable grommets must be used for wiring.

#### Information:

**To meet UL safety certification requirements for this product, the SiteManager must be mounted at a location with restricted access.**

### 3.2.8 Initial configuration via controller

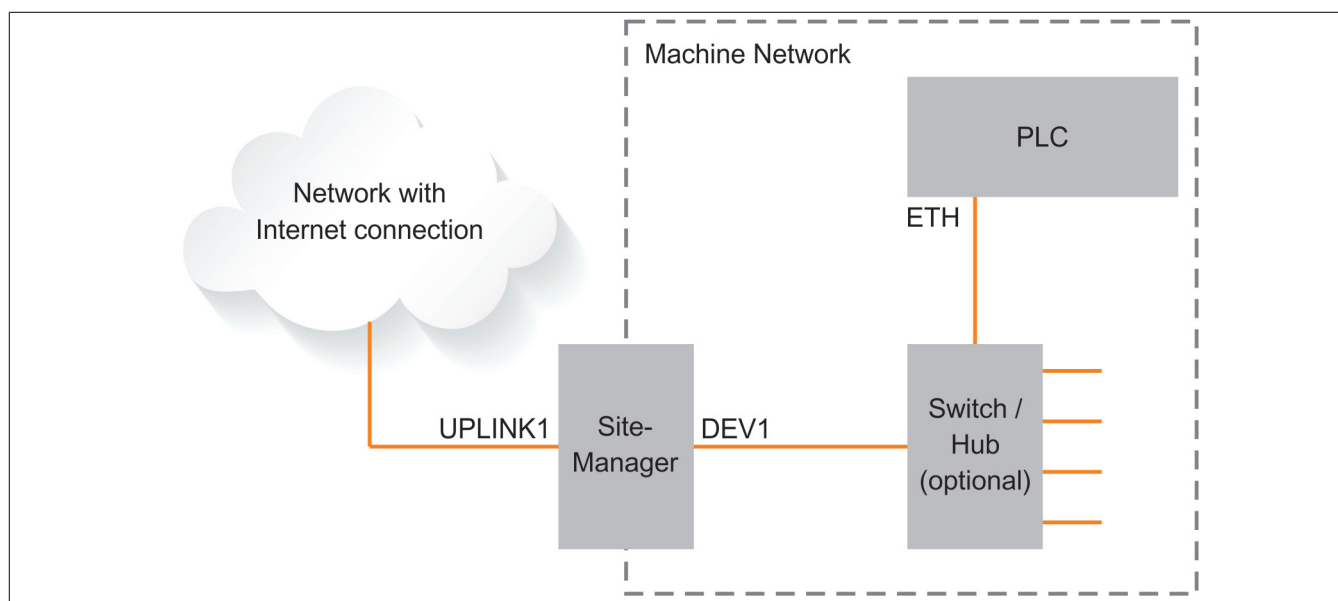
In its unconfigured state (factory settings) a SiteManager is configured via the controller. To do this, the SiteManager must be added to the Automation Studio project on the desired Ethernet interface of the controller. In the event that the SiteManager needs to be replaced later on, this allows the most important settings to be restored in order to establish a remote maintenance connection.

The initial configuration by the controller is also required so that register "ModuleOK" for I/O mapping can carry out its function.

For the controller to configure the SiteManager automatically, the DEV1 port must be connected to an Ethernet interface on the controller. There is not permitted to be a routed network in between them. Only an Ethernet switch or hub is permitted.

A SiteManager module ID is only permitted to be used once on the controller's interfaces and throughout the entire Layer 2 network. In order to use multiple SiteManagers, they must have different module IDs.

#### Network diagram



#### 3.2.8.1 Ethernet configuration

##### Interface on the controller

The network interface on the controller must be configured with a private IPv4 address.

- 10.x.x.x
- 172.16.x.x
- 192.168.x.x

If an invalid IP address is used, the SiteManager cannot perform the automatic configuration for security reasons.

##### DEVx port of the SiteManager

The DEVx port must be in the same subnet as the interface on the controller; otherwise, static routes must be set.

### 3.2.9 SiteManager\_1315-1335-1345 - Initial setup

#### 3.2.9.1 Configuring UPLINK settings for internet access

The SiteManager must be able to access the Internet via an UPLINK port in order to access a GateManager server. It receives its IP address via DHCP by default; only the uplink settings must be configured manually if a static IP address is used on the Ethernet interface (UPLINK1) or if a USB broadband modem should be used as UPLINK2.

The following 5 methods are available:

##### 3.2.9.1.1 Using Automation Studio

- a) For details, see "Secure Remote Maintenance" in ["Automation Studio" on page 35](#).

##### 3.2.9.1.2 Using Appliance Launcher

- a) Download [Appliance Launcher](#) from the B&R website and install it.
- b) Connect the DEV1 or UPLINK1 port of the SiteManager to the local network and switch it on. The SiteManager must be on the same subnet as the PC. Alternatively, the SiteManager can be connected directly to the PC with an Ethernet cable.
- c) Switch on the SiteManager and wait approx. 1 minute for it to become ready for operation.
- d) After Appliance Launcher is started, the SiteManager should be listed on the first screen. If it does not appear immediately, press the Search button a few times. (It is important to note that Appliance Launcher will only display the SiteManager if the PC has a true private IP address (10.x.x.x, 172.16-31.x.x, 192.168.x.x, or 169.254.x.x)).
- e) Follow the wizard and set the UPLINK1 address if a static IP address should be used, or go to the UPLINK2 menu to set the SSID/Wi-Fi key for an integrated or optional USB Wi-Fi module or define a PIN code for an integrated or optional broadband modem.
- f) For additional information about the GateManager settings, see ["Settings for GateManager server connection" on page 33](#).

##### 3.2.9.1.3 Using the standard IP address (10.0.0.1)

- a) Connect the DEV1 port of the SiteManager to the Ethernet interface of the PC using a standard Ethernet cable.
- b) Configure the Ethernet adapter of the PC to 10.0.0.2, subnet mask 255.255.255.0.
- c) Switch on the SiteManager and wait approx. 1 minute for it to become ready for operation.
- d) Enter the following in the web browser: `https://10.0.0.1`.
- e) Log in with username **admin** and use the MAC address of the SiteManager as the password (printed on the label).
- f) Open menu **System > UPLINK1** to set the UPLINK1 address if a static IP address should be used, or open menu **UPLINK2** to set the SSID/Wi-Fi for an integrated or optional USB Wi-Fi module or a PIN code for an integrated or optional broadband modem.
- g) For additional information about the GateManager settings, see ["Settings for GateManager server connection" on page 33](#).

##### 3.2.9.1.4 Using a DHCP server

- a) Connect the UPLINK port of the SiteManager to the local network and switch it on.
- b) After approx. 1 minute, the SiteManager should have received an IP address from the DHCP server.
- c) Check the DHCP server's lease list to find out the IP address.
- d) Enter the IP address in your web browser with preceding `https://` (e.g. `https://192.168.41.13`).
- e) Log in with username **admin** and use the MAC address of the SiteManager as the password (printed on the label).
- f) Open menu **System > UPLINK1** to set the UPLINK1 address if a static IP address should be used, or open menu **UPLINK2** to set the SSID/Wi-Fi for an integrated or optional USB Wi-Fi module or a PIN code for an integrated or optional broadband modem.
- g) For additional information about the GateManager settings, see ["Settings for GateManager server connection" on page 33](#).

### 3.2.9.1.5 Using a USB flash drive

- a) Log in to the GateManager portal with the admin account and locate the domain to which the SiteManager should connect.
- b) Click on the "USB configuration" symbol and set the **UPLINK1** or **UPLINK2** port. Nothing must be configured if the SiteManager is connected to a local intranet with a DHCP server.
- c) Click on "Create" to save the configuration file locally on the PC.
- d) Copy the configuration file to a USB flash drive formatted with FAT32.
- e) Switch on the SiteManager and wait until the SiteManager is ready (status no longer blinking).
- f) Connect the USB flash drive and wait until the SiteManager has automatically rebooted. If the SiteManager has access to the GateManager, the LED status indicator should be green.
- g) Remove the USB flash drive. No further configuration is required.

### 3.2.9.2 Settings for GateManager server connection

- 1) In the SiteManager web-based user interface, go to menu **GateManager > General** menu (if using Appliance Launcher, follow the wizard for the GateManager parameter page).
- 2) Enter the **IP address** of the **GateManager** server to which the SiteManager should connect and a **domain token** for the domain where the SiteManager should appear. This information should be provided by the administrator or entity from which the SiteManager was obtained. This information is also listed in the bottom section of the account emails sent by GateManager.
- 3) The LED status indicator is constantly green, which means that the SiteManager is connected to the GateManager.
- 4) As soon as the SiteManager is connected to the GateManager, the GateManager admin or LinkManager client account can be used to gain remote access to the SiteManager web-based user interface to perform additional configuration (DEV ports, agents, etc.).
- 5) Detailed instructions, new firmware, etc. can be downloaded from <http://www.br-automation.com/sitemanager>.

### 3.2.9.3 Internet access with integrated broadband

#### Information:

This section is only valid for variant 1x35.

The broadband modem connection is called UPLINK2. The SiteManager always attempts to use the Ethernet connection (UPLINK1) by default. UPLINK2 is used only if the Internet connection is lost on UPLINK1. As soon as a connection to UPLINK2 is established, a switch to UPLINK1 is not made until the next restart or if the Internet connection to UPLINK2 is lost.

If the modem uses a SIM PIN code, the PIN code should be entered in menu **System > UPLINK2** of the SiteManager. The SiteManager automatically detects the access point name (APN) from an internal table. This can also be entered manually via menu **UPLINK2**, however.

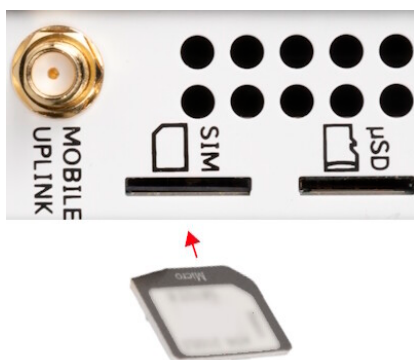
If the SIM card used does not have a PIN code, no further configuration of UPLINK2 is required in the SiteManager. (The PIN code can be removed from a SIM card by inserting it into a standard cell phone and using the phone's "Remove SIM card" function.)

In order to reduce the data traffic, you can configure UPLINK2 so that the mobile network connection changes to the sleep mode when not in use. The connection is restored when an SMS text message is sent to the phone number on the SIM card.

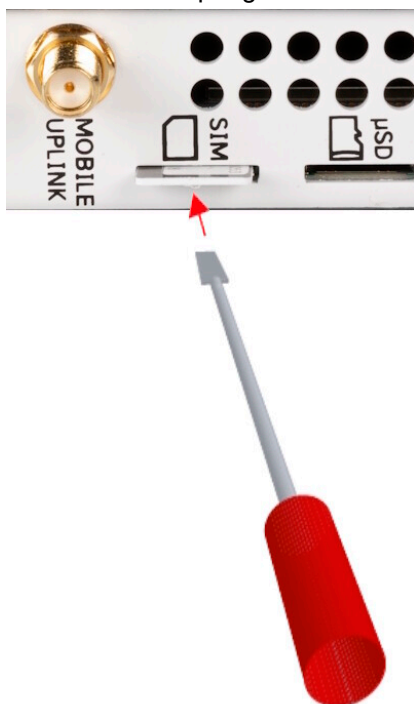
## Inserting a SIM card

A 3DD micro-SIM card (12 x 15 mm) is required. The SIM card must be used as follows:

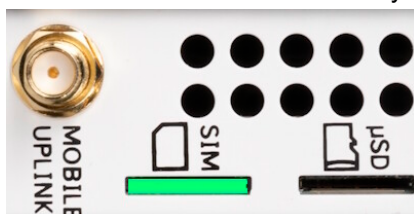
- Slide the SIM card into the slot.



- Use a narrow object, such as a screwdriver, to push the SIM card further into the slot (approx. 2 mm) until the click of the spring lock is heard.



- The SIM card is inserted correctly when it is flush with the SiteManager housing.



### 3.2.9.4 Internet access with integrated Wi-Fi module

#### Information:

This section is only valid for variant 1x45.

The SiteManager can connect to a Wi-Fi access point via the integrated Wi-Fi module. The connection is called **UPLINK2**.

When activating the Wi-Fi client, SiteManager will try to connect using "sitemanager" as the SSID and the MAC address of SiteManager as the Wi-Fi key by default.

The SSID and Wi-Fi key can be configured in menu **System > UPLINK2**.

### 3.2.10 Automation Studio

#### Information:

The different variants of the SiteManager have fixed device IDs in Automation Studio. Only one SiteManager of each variant is therefore permitted to be used per CPU module.

#### Information:

By default, ports 50000 and 51000 are enabled for connecting and configuring B&R "safety technology" modules using a B&R Secure Remote Maintenance solution. These ports can be used to send data from Automation Studio to safety modules (e.g. configuration) and to receive data from them (e.g. status information).

In Automation Studio, it is possible to freely define the port number of a safety module. If a port number is set that is not the enabled by default in the SiteManager for Secure Remote Maintenance (50000 or 51000), then these ports must be enabled in the SiteManager.

A new B&R agent (under Agents) must be created via the SiteManager user interface, which must include a port expansion with the port number set in the safety module.

#### 3.2.10.1 Function model "Standard"

##### I/O mapping register overview

Register	Name	Description	Data type	Read		Write	
				Cyclic	Acyclic	Cyclic	Acyclic
0	<a href="#">ModuleOK</a>	Module status (1 = Module inserted)	BOOL	•			
4	<a href="#">SerialNumber</a>	Serial number	UDINT	•			
10	<a href="#">ModuleID</a>	Module ID	UINT	•			
16	<a href="#">ConfigurationMismatch</a>	Parameters for the main configuration changed	BOOL	•			
0	<a href="#">RefreshCnt01</a>	Request counter	UINT	•			
4	<a href="#">RemoteManagement01</a>	Current value for remote management	USINT	•			
5	<a href="#">ConnectionStatus01</a>	Current connection status	USINT	•			
8	<a href="#">StatusUPLINK1</a>	Status of the UPLINK1 port	USINT	•			
9	<a href="#">StatusUPLINK2</a>	Status of the UPLINK2 port	USINT	•			
10	<a href="#">StatusUPLINK3</a>	Status of the UPLINK3 port	USINT	•			
11	<a href="#">StatusUPLINK4</a>	Status of the UPLINK4 port	USINT	•			
12	<a href="#">StatusDEV1</a>	Status of the DEV1 port	USINT	•			
13	<a href="#">StatusDEV2</a>	Status of the DEV2 port	USINT	•			
14	<a href="#">StatusDEV3</a>	Status of the DEV3 port	USINT	•			
15	<a href="#">StatusDEV4</a>	Status of the DEV4 port	USINT	•			
16	<a href="#">RemoteManagementControlFlags01</a>	Status bits for remote management control	USINT	•			
0	<a href="#">RemoteManagementControl01</a>	Control of remote access (overwrites RemoteManagement01)	USINT			•	
1	<a href="#">RemoteManagementControlEnable01</a>	Enable remote management control	BOOL			•	

##### Automation Studio main configuration

The main configuration includes all the settings needed to establish a connection from the SiteManager to the GateManager. Transfer to the SiteManager is initially possible one time (see ["Initial configuration via controller" on page 31](#)). To re-transfer the SiteManager configuration, press and hold the reset button for at least 5 seconds.



The following table shows the parameters of the main configuration that can be accessed via Automation Studio:

Parameter	Description
DEV1 port <sup>1)</sup>	
IP address	IP address of the DEV1 port on the SiteManager
Subnet mask	Subnet mask of the DEV1 port on the SiteManager
UPLINK1 port	
Mode	Mode of the UPLINK1 port: DHCP or static (enables the following 4 entries)
IP address	IP address of the UPLINK1 port on the SiteManager (mode = Static)
Subnet mask	Subnet mask of the DEV1 network on the SiteManager (mode = Static)
Default gateway	Default gateway (mode = Static)
DNS server	DNS server address, when hostname for GateManager or proxy is used (mode = Static)
UPLINK2 port (only for device variants 1x35 and 1x45)	
Integrated modem (1x35) Wi-Fi module (1x45)	Enable/Disable the UPLINK2 port (enables 2 of the following entries, depending on the variant)
APN (1x35)	Access Point Name (UPLINK2 = Mobile network)
SIM PIN code (1x35)	SIM PIN code (UPLINK2 = Mobile network)
SSID (1x45)	WLAN network name (UPLINK2 = Wi-Fi)
Wi-Fi KEY (1x45)	Wi-Fi key (UPLINK2 = Wi-Fi) For security reasons, WLAN networks are protected with a password. An ASCII character string with a minimum of 8 and maximum of 63 characters must be entered.
GateManager settings	
Remote management <sup>1)</sup>	<p>GateManager access Controls connection setup between the SiteManager and GateManager. The following options can be selected (see also "<a href="#">RemoteManagement01</a>" on page 37):</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Do not connect to the GateManager. All remote maintenance and management options will be disabled (similar to switching off the respective SiteManager).</li> <li>• <b>Heartbeat only:</b> Connect to the GateManager, but only to send periodic status information and optionally provide a connection to the SiteManager itself (if permitted by settings "Go To Appliance").</li> <li>• <b>Enabled:</b> Connect to the GateManager and allow remote access to the SiteManager (if permitted by "Go To Appliance" settings) and connected devices.</li> <li>• <b>Heartbeat and relays only:</b> Connect to the GateManager with static device and activated server relay, but only to send periodic status information and optionally provide a connection to the SiteManager itself (if permitted by "Go To Appliance" settings).</li> </ul>
Go To Appliance <sup>1)</sup>	<p>Displays the connection options for accessing the SiteManager's user interface. This option specifies if and how a GateManager administrator or LinkManager user is able to use function "Go to appliance" to connect to the SiteManager's user interface (this cannot be set via Appliance Launcher):</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Access to "Go To Appliance" is blocked.</li> <li>• <b>Manual Login:</b> When using "Go To Appliance", the normal login data (user and password) for the SiteManager must be entered in order to log in to the SiteManager.</li> <li>• <b>Automatic login:</b> When using "Go to appliance" in the GateManager portal or in the LinkManager console domain view, the dynamic password generated by the GateManager can be used. If the GateManager console is configured for automatic login, the login data is provided to the SiteManager automatically. If the GateManager console is configured for manual login, the login dialog box appears.</li> <li>• <b>Manual, not LinkManager:</b> Like manual login, but "Go To Appliance" is not possible from the LinkManager console domain view.</li> <li>• <b>Automatic, not LinkManager:</b> Like automatic login, but "Go To Appliance" is not possible from the LinkManager console domain view.</li> </ul>
Appliance name	<p>Name of the device on the GateManager server with a maximum of 127 characters. This name is used by the GateManager administrator to identify the respective SiteManager. The value in this field corresponds with the %N field code from the device name format specifications. According to the default device name format, if this field is empty, then the <b>Device Name</b> is used. If that is also empty, the SiteManager serial number is used.</p>
Domain token	<p>Domain on the GateManager server with a maximum of 127 characters (including spaces and decimals) The domain token is only used to establish the first connection. If a multiple-domain account is used and a complete domain token requires 48 or more characters, a higher-level token must be used (e.g. TOPLEVEL.INTERNATIONAL.AUSTRIA.EGGELSBURG).</p>
GateManager address	<p>Address of the GateManager server (IP address or DNS hostname) If it is an alternative IP address for accessing the same GateManager server, then both addresses should be entered here, separated by a space. If using Appliance Launcher to configure the GateManager, the DNS button must be pressed so the two IP addresses can be entered (separated by a space).</p>
Proxy settings	
Proxy	Enable/Disable proxy settings (enables the following 3 entries)
Web proxy address	<p>Proxy address for the GateManager connection (IP address or hostname) The IP address (and optionally the port number separated by a colon) of the web proxy via which the SiteManager should connect to the GateManager. Alternatively, a web proxy auto-discovery (WPAD) URL can be specified, from which the SiteManager can obtain the actual web proxy address, e.g. <a href="http://172.16.1.1:8080/wpad.dat">http://172.16.1.1:8080/wpad.dat</a>.</p>
Web proxy user	Proxy username
Web proxy password	Proxy password

1) The settings of the DEV1 port are applied to DEV2 and DEV3. For additional details, see "[Default settings](#)" on page 28.

2) These Automation Studio project parameters are not verified and can be changed later on using the web-based user interface on the SiteManager.



### 3.2.10.1.1 ModuleOK

Status bit that indicates whether the module is physically present and configured. Detection takes place via the fieldbus connection.

Data type	Values	Information
BOOL	0	Module not ready for operation
	1	Module present and configured

### 3.2.10.1.2 ModuleID

The module hardware ID used to determine the type of device can be read from this register. This is also listed in the respective technical data as the "B&R ID code". In addition, a serial number is printed on each module; the module hardware ID corresponds to the first 4 positions of this serial number.

Data type	Values
UINT	0 to 65535

### 3.2.10.1.3 SerialNumber

The module's unique serial number can be read from this register. This 7-digit serial number is printed in decimal form on the module's housing.

Data type	Values
UDINT	0 to 4,294,967,295

#### Information:

##### Module serial number

The complete module serial number is made up of the 4-digit ModuleID and subsequent 7-digit SerialNumber.

##### Example:

- ModuleID = 0xE908
- SerialNumber = 0x0001234
- Serial number printed on the module = 0xE9080001234

### 3.2.10.1.4 ConfigurationMismatch

This data point can be used to determine if a parameter in the main configuration has been changed.

A list of all parameters that are checked is provided in the main configuration table in Automation Studio, see ["Automation Studio main configuration" on page 35](#).

Data type	Value	Information
BOOL	0	The Automation Studio project configuration is identical to the configuration on the SiteManager.
	1	At least one parameter in the main configuration on the device has been changed or the Automation Studio project configuration does not match the configuration on the device.

### 3.2.10.1.5 RefreshCnt01

The request counter is incremented by 1 after every time the status information is read.

Data type	Values
UINT	0 to 65535

### 3.2.10.1.6 RemoteManagement01

Current value of the "Remote management" setting. Defines the connection setup from the SiteManager to the GateManager.

Data type	Value	Name	Information
USINT	0	Disabled	Remote maintenance access disabled
	1	Heartbeat only	Connection check with GateManager
	2	Enabled	Remote maintenance access enabled
	3	Heartbeat and relays only	Connection check and relays enabled
	4 to 255	-	Reserved

### 3.2.10.1.7 ConnectionStatus01

Status of the current GateManager connection:

Data type	Value	Information
USINT	0	NC
	1	GateManager connection OK (Heartbeat OK)
	2	Remote maintenance connection active (access via LinkManager)
	3 to 255	Reserved

### 3.2.10.1.8 StatusUPLINK1 to 4

Status of the respective UPLINK port. The actual number of UPLINK ports depends on the device variant:

Data type	Value	Information
USINT	0	DOWN
	1	UP, default interface
	2	UP, secondary interface
	3 to 254	Reserved
	255	Not installed

### 3.2.10.1.9 StatusDEV1 to 4

Status of the respective DEV port:

Data type	Value	Information
USINT	0	DOWN
	1	10 Mbps HDX
	2	10 Mbps FDX
	3	100 Mbps HDX
	4	100 Mbps FDX
	5	Reserved
	6	1000 Mbps FDX
	7 to 254	Reserved
	255	Not installed

### 3.2.10.1.10 RemoteManagementControl01

Controls connection setup from the SiteManager to the GateManager. This data point can be used to overwrite the value of setting "Remote management".

Data type	Value	Name	Information
USINT	0	Disabled	Remote maintenance access disabled
	1	Heartbeat only	Connection check with GateManager
	2	Enabled	Remote maintenance access enabled
	3	Heartbeat and relays only	Connection check and relays enabled
	4 to 255	-	Reserved

### 3.2.10.1.11 RemoteManagementControlEnable01

Enable remote management control.

The desired value must first be set using the data point [RemoteManagementControl01](#).

Data type	Value	Information
BOOL	0	Switch off RemoteManagementControl.
	1	Switch on RemoteManagementControl.

After RemoteManagementControlEnable01 has been reset to FALSE, setting "Remote management" returns to the originally configured value.

### 3.2.10.1.12 RemoteManagementControlFlags01

Status bits for remote management control:

Data type	Bit	Name	Information
USINT	0	RemoteManagementControlAck01	Acknowledgment of RemoteManagementControlEnable01
	1	RemoteManagementControlStatus01	Status of remote management control (0 = OK)
	2 to 7	-	Reserved

#### RemoteManagementControlAck01

This bit is used to check if the action set with [RemoteManagementControlEnable01](#) has been completed. If RemoteManagementControlAck01 takes on the value of [RemoteManagementControlEnable01](#), transfer has been carried out. It is then possible to read RemoteManagementControlStatus01 to determine if the operation was successful.

#### RemoteManagementControlStatus01

This bit is set when an error occurs while enabling/disabling remote management control. This may be caused by the following:

- Value of RemoteManagementControl01 data point is invalid
- Network connection was lost

### 3.2.10.2 Operating function model "Standard"

The "Remote management" configuration parameter can be used to set the connection type permitted by the SiteManager. This value can be controlled at runtime.

To do this, the desired value must first be set using the RemoteManagementControl01 data point. Then remote management control is enabled by setting RemoteManagementControlEnable01 to TRUE. Once RemoteManagementControlAck01 has changed to TRUE, RemoteManagementControlStatus01 can be used to check whether the change has been applied successfully.

Resetting RemoteManagementControlEnable01 to FALSE resets "Remote management" back to the original value of the configuration parameter.

### 3.2.11 Connecting to the GateManager

By default, a SiteManager automatically tries a number of different methods and protocols to connect to a GateManager address. The preferred connection method can be set in the SiteManager configuration.

#### Information:

**Access to the GateManager from the SiteManager must be enabled through the end customer's firewall. The SiteManager supports proxy servers that enable this access to be regulated more exactly.**

- ACM/PXP (Port 11444 TCP): This is a dedicated port for connecting to the GateManager server. Using a dedicated port is normally preferred because it separates GateManager-related traffic from other outgoing traffic on the network, making it easier to track GateManager traffic on the local network and on the Internet connection. Using a dedicated port also means that this port must probably be opened in the corporate firewall, however, which may violate corporate policies.
- HTTPS/TLS (port 443 TCP): This connects to GateManager using the TLS protocol on port 443. This should work through firewalls that allow outgoing HTTPS connections.
- TLS over HTTP (port 80 TCP): The connection to the GateManager is established over the standard HTTP port 80 but immediately converted to a secure TLS connection. This can work through a firewall that only permits outgoing HTTP connections.
- TLS via web proxy: This establishes a connection over a specified web proxy and requests the web proxy to connect to the GateManager over port 443 TCP. As soon as the connection is established, the normal TLS protocol is used.
- HTTP via web proxy: The connection is made through a specified web proxy; the web proxy is asked to connect to the GateManager over port 80 TCP. As soon as the connection is established, it is switched to a secure TLS connection.

#### Additional outgoing connections

In addition, the SiteManager looks for 193.242.155.50-59 port 80 and asks whether the GateManager address is known. This is a built-in function of the SiteManager as a service to the end user. If a customer has its own GateManager with public IP address xx.xx.xx.xx, for example, but needs to change it to xx.xx.yy.yy. B&R can create the "NATting" in the GateManager discovery service in this case, which says that SiteManagers connecting to xx.xx.xx.xx should connect to xx.xx.yy.yy.

#### Connecting to the GateManager for the first time

When the SiteManager connects to a GateManager for the first time, the SiteManager requests the "Appliance TLS X.509 certificate" from the GateManager. This is a unique self-signed certificate. The SiteManager initiates a TLS handshake with the GateManager. After a successful first handshake, the SiteManager is connected to the GateManager's unique "Appliance TLS X.509 certificate". Since the SiteManager is now bound to the GateManager's unique certificate, it is secure against MITM/redirect attacks.

### 3.3 LinkManager

The LinkManager is an easy-to-install Windows application that runs on the service technician's PC. The LinkManager connects via 2-factor authentication to the GateManager and, together with the SiteManagers, enables secure access to remote devices. Once connected, it makes the remote device appear to the field engineer as if the Windows PC was connected directly to the device and it is possible to establish connections to the remote device via FTP, web, RDP, VNC or Automation Studio.

A browser-based and reduced version of the LinkManager is also available with the LinkManager Mobile variant. No software must be installed in order to use LinkManager Mobile. LinkManager Mobile runs on every operating system (Windows, iOS, Android, Mac and much more). It supports Internet, RDP and VNC protocol connections.

#### Information:

**Max. 10 simultaneous LinkManager connections are possible via a SiteManager.**

#### Information:

**For a connection via VNC protocol, a dedicated VNC agent must be used (dedicated address and port number, e.g. 192.168.0.8:5910).**

#### 3.3.1 Order data

Model number	Short description
0RMLM.MOB	Secure remote maintenance - LinkManager mobile license, individual license, non-floating, independent of operating system
0RMLM.WIN	Secure Remote Maintenance - LinkManager license, shared license (floating license), Win XP/7/8/10/11 <sup>1)</sup>

Table 12: 0RMLM.MOB, 0RMLM.WIN - Order data

1) Windows 11 support in version 9.7.x and later

#### Information:

**Download the LinkManager software via <http://www.br-automation.com/linkmanager>.**

### 3.4 Starter package

A starter package is helpful for quick entry into the remote maintenance solution. It contains the following components:

- **GateManager:** 1x GateManager with hosting agreement
- **SiteManager:** 1x any SiteManager model or 1x SiteManager Embedded variant
- **LinkManager:** 1x LinkManager license and 1x LinkManager Mobile license
- **Service agreement**

The core of a starter package is access to a GateManager provided and administered by B&R (GateManager hosting service). It can then be used by customers to manage their own SiteManager and LinkManager.

A starter package can be extended as required, e.g. by switching to a different service level or purchasing additional LinkManager licenses and SiteManagers. Migrating from the GateManager hosting service to a separate GateManager (hardware or software variant) is also possible at any time.

#### 3.4.1 Order data

Model number	Short description
	<b>SiteManager</b>
0RMGMZSP.1315	GateManager hosting service - "Starter" package, includes 1x SiteManager, 1x LinkManager and 1x LinkManager Mobile license, service fee 0RMAS.SERVICE-01 must be paid separately.
0RMGMZSP.1335	
0RMGMZSP.1335.4G	
0RMGMZSP.1345	
0RMGMZSP.SME.B	GateManager hosting service - "Starter" package, includes 1x SiteManager embedded BASIC license, 1x LinkManager and 1x LinkManager Mobile license, service fee 0RMAS.SERVICE-01 must be paid separately.
0RMGMZSP.SME.E	GateManager hosting service - "Starter" package, includes 1x SiteManager embedded EXTENDED license, 1x LinkManager and 1x LinkManager Mobile license, service fee 0RMAS.SERVICE-01 must be paid separately.

### 3.5 Network safety

Communication between the components of the remote maintenance solution is based on SSL VPN with AES encryption. The LinkManager communicates with the SiteManager exclusively via the GateManager. The LinkManager and SiteManager register themselves via 2-factor authentication on the GateManager.

2-factor authentication is based on an X.509 certificate. Each GateManager is capable of generating unique TLS certificates to which a SiteManager binds itself. This connection is established once and can only be lifted by the GateManager or SiteManager, which makes a man-in-the-middle attack impossible. Alternatively, authentication via SMS can be used for the LinkManager.

The SiteManager can be configured so that it transfers information in cyclic intervals (standard setting 10 min) to the GateManager (keep-alive signal). In addition, remote access can also be physically controlled by the machine operator. This is possible by interrupting the power supply or via a switch on the digital input that interrupts or permits the connection to the GateManager.

An important factor in network security is the integrated firewall in the SiteManager. The firewall is configured with "device agents", which correspond to firewall rules. A device agent can be used to define which protocol and via which ports access to a network station is permitted. The device agent then only permits access to this one network station. In addition, the device agents can also be assigned to LinkManager users. This also allows exact access control on the user level.

The remote maintenance solution fulfills all security standards that were specified by the "National Institute of Standards and Technology" ([www.nist.gov](http://www.nist.gov)) for encryption and key transfer.

#### Information:

**To achieve maximum IT security, it is strongly recommended to always use the current GateManager, SiteManager and LinkManager software versions.**

### 3.6 Port information

#### SiteManager and LinkManager

These connect to the public IP address of the GateManager server via TCP port 11444 (Secomea ACM /TLS), 443 (standard HTTPS/TLS) or 80 (standard TLS over HTTP). When using an Internet firewall / NAT router, it must be configured so that all incoming connections are forwarded to the GateManager server's private IP address via a static public IP address, port 11444 (or 443 or 80).

#### GateManager administrator web portal

This connects to the GateManager server via TCP port 443.

#### Information:

**If the web portal is located behind a NAT router, the router is not permitted to mask incoming connections. The GateManager must always be able to determine the IP address of the original source.**

The administrator web portal allows the administrator to access the web interface of SiteManager, LinkManager and web-enabled devices connected to SiteManager. This function uses the TCP port range 55000 to 59999. To use this function externally, the NAT router must be configured to forward incoming connections to the appropriate ports on the GateManager server.

#### Ports for LinkManager Mobile

The following outgoing ports must be open for LinkManager Mobile to work:

Port	Protocol	Description
80	TCP	HTTP
443	TCP	HTTPS

The following outgoing ports must be open to use an external application with LinkManager Mobile.

Port	Protocol	Description
22	TCP	SSH
3389	TCP	RDP
5800	TCP	JVNC
5900	TCP	VNC

#### Installing the GateManager

Additional ports and services are used when installing the GateManager. These are described in the "GateManager 8250 setup guide" and have no effect on the users of the hosted service, for example.

## 4 Getting started with the system components

The following steps are a guide through the most important additional documentation and user tips (see "[Additional documentation](#)" on page 51) for setting up the GateManager, SiteManager and LinkManager for first use.

### GateManager

#### Information:

The steps in this section are necessary if the GateManager is not hosted by B&R.

In the event that the hosted service is used, access only has to be requested from B&R in order to receive an email with the GateManager address and access data for activation (certificate and password).

1. If the software installer is used as the GateManager server, then the instructions from the following documents must be followed to install the software:
  - [GateManager 8250 Setup Guide - Red Hat Enterprise Linux](#)
  - [GateManager 8250 Setup Guide - Debian](#)
  - [Setup Guide Postfix SMTP Relay](#)
  - [GateManager Commands](#)

#### Notice!

Some documents contain links or instructions for software downloads from the Secomea website. These are not permitted to be used; the download MUST ALWAYS be from the B&R website.

#### Information:

A GateManager that was set up with the named documents is now ready for operation with all functions but only in test/demo mode for the moment (max. 3 SiteManager can be managed). To use the GateManager to its full extent, it must be activated accordingly. See "[Activating the GateManager](#)" on page 16.

2. Refer to the instructions in document [Getting started GateManager PREMIUM domain administration](#) to configure the GateManager software and to create and manage domains (see also "[Managing domains and their content](#)" on page 45).

### SiteManager

1. Follow the instructions from the information sheet ([SiteManager 1115-1135-1145 Initial Setup](#) or from section "[SiteManager\\_1315-1335-1345 - Initial setup](#)" on page 32 to configure the SiteManager and make the settings necessary for the Internet connection and the connection to the GateManager server. The following download option is also available for Appliance Launcher: [Appliance Launcher](#)
2. If SiteManager is configured using Automation Studio, see Automation Help for the SiteManager or section "[Automation Studio](#)" on page 35.



## Managing domains and their content

### Information:

The **GateManager** is the point where the **LinkManager** user and the **SiteManager** are managed.

Users and licenses can be subsequently managed within the domains.

Separate accounts must be set up for GateManager administrators and LinkManager users.

Device agents can be set up on a device. A device agent can be either a PLC or a rule set. Device agents therefore enable access to network participants on the device network of the SiteManager.

The "SiteManager GUI" button in the GateManager can be used to open the web interface of the selected SiteManager. The agents can be suitably created for the separate devices in the section **GateManager ► Agents**.

### LinkManager Mobile users

LinkManager Mobile allows users remote access to industrial equipment from their iPhone, iPad or Android device. The app is designed to access graphical user interfaces such as PLC devices, HMI control panels or webcams. It also connects to desktops running Linux or Windows. LinkManager Mobile can be used to easily connect with the device, start a VNC or MS Remote Desktop (RDP) client and then control the device remotely.

### LinkManager 7

### Information:

This product is no longer maintained, and no new security updates are available.  
A version change to LinkManager should therefore be carried out.

### LinkManager 8 and higher

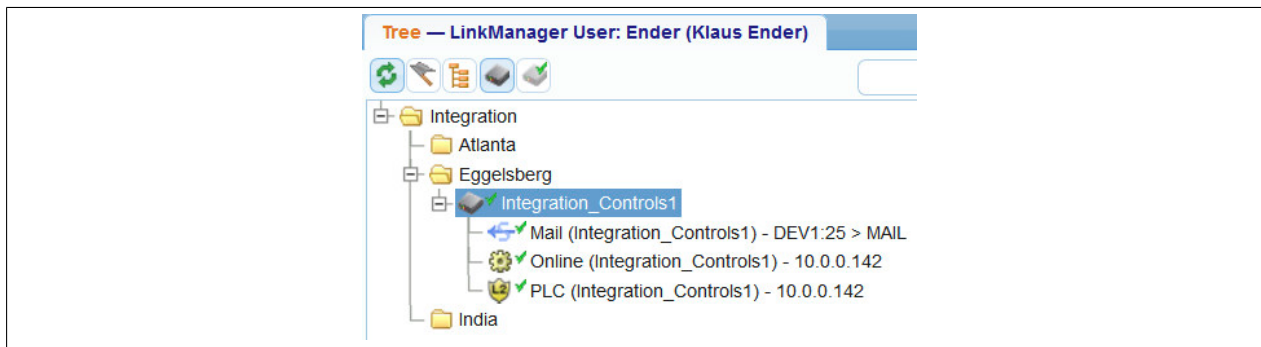
### Information:

In order to use the LinkManager, an email with the access data (LinkManager user certificate and associated account password) must be sent by the GateManager administrator.

1. If not already done, install the LinkManager. The LinkManager can also be downloaded here: <http://www.br-automation.com/linkmanager>.

The screenshot displays the GateManager web interface. On the left, under the heading "GateManager", there is a section titled "Select a GateManager Service:". It contains three options, each with an icon and a button: "GateManager Portal" (with a server rack icon), "LinkManager" (with a person at a laptop icon), and "LinkManager Mobile" (with a person at a tablet icon). On the right, there is a "Remote Maintenance LinkManager" header with an icon of two people. Below this is the "GateManager Login" section, which includes two radio buttons: "Certificate:" (unselected) and "User name:" (selected). The "User name:" field contains the text "Ender". Below it is a "Password:" field with masked characters. A "Login" button is located at the bottom of the login section.

- Open a browser window and navigate to the GateManager (IP address or hostname). Then select entry "LinkManager". A browser window will open where the LinkManager user certificate or username and account password for LinkManager will be entered.



- After logging in, the present domain is displayed.



- The individual agents can now be accessed with the LinkManager.
- For additional information about LinkManager 8, see [here](#).

## 5 Migrating to a new SiteManager version

This guide presents various scenarios for the migration process from a discontinued SiteManager variant (e.g. 1135 3G/4G regional variants or 11xx versions) to SiteManager 13xx. Other procedures may also work, such as updating the project via a USB flash drive, but have not been tested.

### 5.1 Products

Order number	Short description
0RMSM1315	Secure Remote Maintenance -SiteManager, LAN 1x Ethernet 100BASE-T uplink connection, 3x Dev connections, 10 device agents, integrated firewall, 2x digital inputs, 2x digital outputs, 24 VDC
0RMSM1335.4G	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T uplink connection, 1x GPRS/3G/4G uplink connection, 3x device connections, 10 device agents, integrated firewall, 2x digital inputs, 2x digital outputs, 24 VDC
0RMSM1345	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T uplink connection, 1x Wi-Fi uplink connection, 3x device connections, 10 device agents, integrated firewall, 2x digital inputs, 2x digital outputs, 24 VDC

### 5.2 Scenarios

In all scenarios, it is assumed that the machine manufacturer would like to use the seamless integration of SiteManager in Automation Studio for reasons of automatic configuration or I/O mapping.

Section "[SiteManager\\_1315-1335-1345 - Initial setup](#)" on page 32 must be taken into account if automatic configuration and the I/O mapping are not used.

#### 5.2.1 Designing new machines

A machine manufacturer would like to design and commission a new machine that uses a SiteManager.

##### 5.2.1.1 Steps for the new configuration

- The new version of the SiteManager must be configured in Automation Studio in "Physical View - System Designer".
- Device agents can be configured manually via the SiteManager user interface or automatically via GateManager "Actions".

#### 5.2.2 Modifying existing machines

A machine manufacturer would like to use the new version of the SiteManager in an existing machine design.

##### 5.2.2.1 Steps for modifying the existing configuration

- Open the current Automation Studio project and replace the currently configured SiteManager with the new SiteManager in Automation Studio in "Physical View - System Designer". This enables automatic SiteManager configuration when the machine is started up by the PLC. The SiteManager configuration does not need to be changed.
- Device agents can be configured manually via the SiteManager user interface or automatically via GateManager "Actions".

#### 5.2.3 Servicing existing systems

A machine manufacturer would like to replace a discontinued variant of the SiteManager with a current SiteManager in an existing system. In this scenario, the SiteManager is defective, the status of the SiteManager is "Down" and it is therefore offline.

#### Information:

**"Monitoring mode" is permanently disabled on all SiteManager variants, i.e. replacing a device does not interfere with machine operation.**

The GateManager (B&R GateManager hosting service or GateManager software) provides an automatic function to replace a SiteManager and restore its configuration. The GateManager automatically saves the SiteManager configuration (network configuration, configured agents and functions such as DCM, usage history and audit logs).

### 5.2.3.1 Steps for modifying the existing plant

#### 5.2.3.1.1 Preconfiguration

- The SiteManager should be preconfigured by the machine manufacturer with the GateManager address, appliance name and domain token before delivery to the end user.
- Depending on who provides the SIM card, the broadband network connection is configured either at the machine manufacturer's or at the end customer's premises.
- To automate the process of preconfiguring multiple SiteManagers, the machine manufacturer can write a dummy PLC application with the correct configuration and thus preconfigure it via Automation Studio / Runtime.
- If the SiteManager was delivered without being preconfigured, the configuration must be made by the service technician at the end user's premises. This is composed of all the configurations above and the broadband network connection for remote connection to the GateManager.

For additional information, see section "SiteManager\_1315-1335-1345 - Initial setup" on page 32.

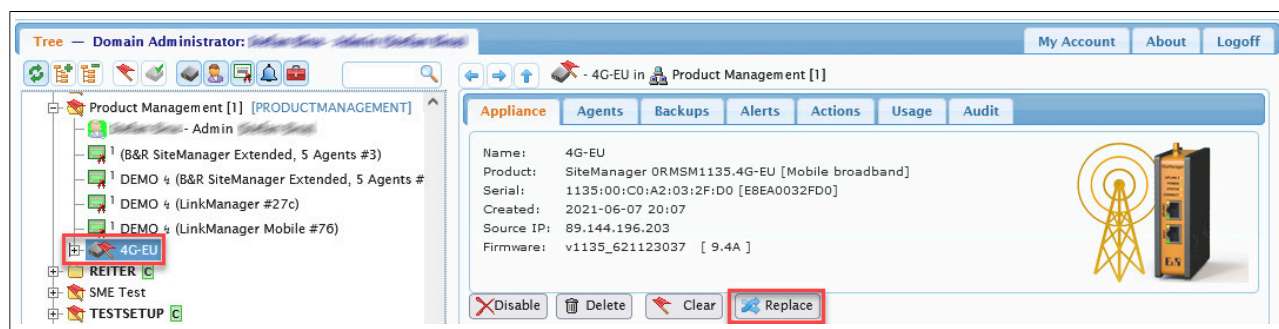
#### 5.2.3.1.2 Replacing the device

In this step, the complete SiteManager configuration (network configuration, configured agents and functions such as DCM) as well as the usage history and audit logs are replicated to the "new" SiteManager.

- Open the GateManager user interface. In the overview of the "old" SiteManager, click on "Replace" and follow the instructions of the GateManager for the process.
- After successful replacement, it takes about 2 to 5 minutes until the correct agents reappear in the GateManager user interface. The obsolete agents can now be deleted.

### Information:

Button "Replace" (see figure) only appears in the GateManager user interface when the SiteManager is offline (after a timeout of 9 min).



#### 5.2.3.1.3 I/O mapping

This step explains how to update the Automation Studio project in order to use the I/O mapping again. If the I/O mapping is not used, this step can be skipped.

- Replace the currently configured SiteManager with the new version of "SiteManager" in Automation Studio in "Physical View - System Designer".
- Establish a LinkManager connection and update the project.
- If flag "ModuleOK" is still False, it is necessary to reset the SiteManager and have the PLC reprogram it so that the PLC accepts the new device. Resetting takes place by pressing the reset button for 5 seconds. Before pressing the reset button, make sure that the SiteManager network configuration is valid in the Automation Studio project. The SiteManager is automatically restarted 2 times during this process.
- After the SiteManager has successfully started up, go to the GateManager user interface to restore the last SiteManager backup. Refreshing the GateManager user interface may be required in order to see the correct appliances/agents configured in the SiteManager.
- To verify correct behavior, connect to the PLC via the LinkManager and check if flag "ModuleOK" is True.

Functions such as "Uplink status" or input "Remote management control 1" will only be accessible again after these steps have been successfully completed.

## 6 SiteManager 4G global SIM card Guideline for USA and Japan

This document contains guidelines for SIM card acquisition, usage, and recommendations for the SiteManager 4G Global model focusing on regions USA and Japan.

### Information:

#### Disclaimer

The information in this document has been gathered and confirmed by our supplier Secomea. B&R does not guarantee that SIM cards from the recommended carriers work or will always be supported, as they have no control over the carriers and their actions.

This guideline is merely a recommendation for customers and partners to make it easier to use the SiteManager 4G global in regions USA and Japan.

### 6.1 Affected material

The guidelines cover the following B&R material:

Order number	Short description
0RMSM1335.4G	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T uplink connection, 1x GPRS/3G/4G uplink connection, 3x device connections, 10 device agents, integrated firewall, 2x digital inputs, 2x digital outputs, 24 VDC

The SiteManager 4G global uses the SIMCom SIM7600G-H modem, which is, a different modem compared to the previously used modems for the region-specific SiteManagers (4G EU/US/JP/CN).

### 6.2 Problem statement and resolution

#### 6.2.1 United States

In the USA, B&R customers and partners generally use the following SIM card provider: AT&T. This does not mean that other SIM card providers will not work with SiteManager 4G Global, however. AT&T is mentioned only because of its network coverage and number of customers. Verizon is one of the largest providers in the US but is not currently supported by B&R.

##### 6.2.1.1 Verizon

The SiteManager 4G Global is not yet certified on Verizon's network as the IMEI is not registered in their system; therefore, we do not yet support SIM cards from Verizon.

##### 6.2.1.2 AT&T

There is a known limitation with AT&T, that SIM cards using some subscriptions are unsuccessful in gaining access to the AT&T 4G network through the SiteManager 4G Global. The reason for this being that the SiteManager 4G Global is not listed in AT&T's IMEI system and is required to be type-approved by AT&T. Therefore, SIM cards are unable to be activated by AT&T for use with the SiteManager 4G Global. Even though the modem itself is certified by AT&T, it is still an ongoing issue with AT&T to connect with some subscriptions requiring AT&T Certified IoT Devices to be used. There are, however, still many Secomea customers in the US who are successfully using AT&T SIM cards ordered online from this marketplace for connecting the SiteManager 4G Global to the 4G network: <https://marketplace.att.com/products/att-iot-dataplans-lte-north-america>. This is therefore the channel recommended by B&R for buying AT&T SIM cards.

There is currently no information about when this limitation will be corrected.

### 6.2.1.3 T-Mobile

Due to changed connection requirements, the SiteManager cannot be used with T-Mobile at the moment, or only with great difficulty.

#### Cause

After T-Mobile closed its 3G network, the company changed the way customers can connect to the 4G mobile network. All devices are expected to be VoLTE-compatible (VoIP over LTE). B&R SiteManagers are not VoLTE-compatible, however.

### 6.2.2 Japan

To use SiteManager 4G Global in Japan, customers will need to choose an MVNO carrier, as the integrated 4G Global modem SIM7600G-H cannot be used with MNO carriers. The reason for this is that SIMCom has not yet acquired MNO carrier connection certification for the SIM7600G-H modem. Therefore, MNO carriers in Japan are cutting off the connection for non-certified modems like the SIM7600G-H and the SiteManager 4G Global is therefore affected by this. Examples of MNOs include NTT Docomo, au, Softbank, and Rakuten, and we do not recommend using these carriers. Instead, we recommend using MVNO carriers.

There are hundreds of MVNO carriers available in Japan, and we cannot verify all of them. However, we have experience using the following MVNO carriers successfully with the 4G Global SiteManager:

IIJ mio	
mineo	
OCN	
BIGLOBE	
Y!mobile	

## 7 Additional documentation

---

User's manuals and data sheets are available for all B&R SiteManager variants and associated GateManager and TrustGate products. Links to the PDF manuals are on the B&R website ([www.br-automation.com/en-gb/products/software/remote-maintenance/](http://www.br-automation.com/en-gb/products/software/remote-maintenance/)) in the general information about the products.

### **Information:**

**The documents on the B&R website refer to Secomea product models and also refer to features, such as a serial or USB interface, that are not available on all B&R SiteManager models.**

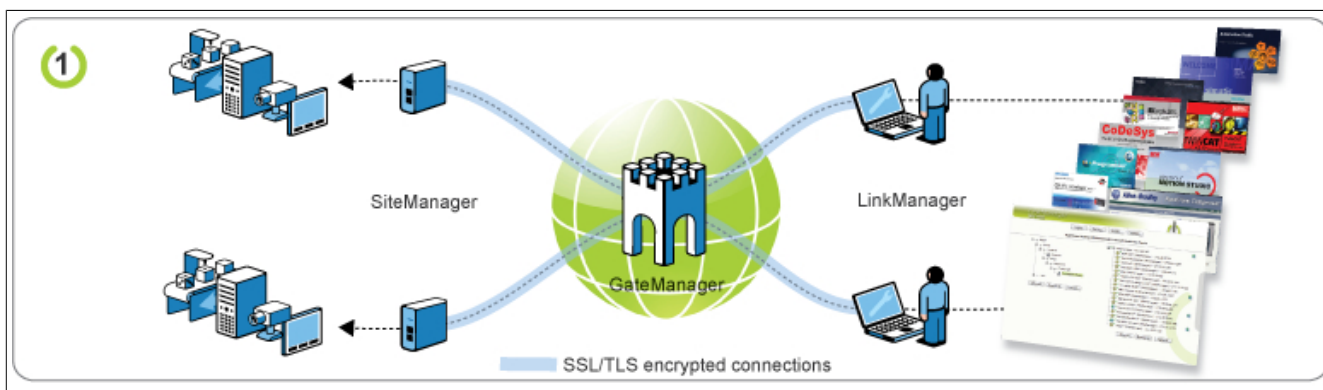


## 8 Use cases and end customer scenarios

This chapter covers various use cases and end customer scenarios and end customer scenarios.

### 8.1 Use cases

#### 8.1.1 Remote maintenance - On-demand access for programming and trouble-shooting

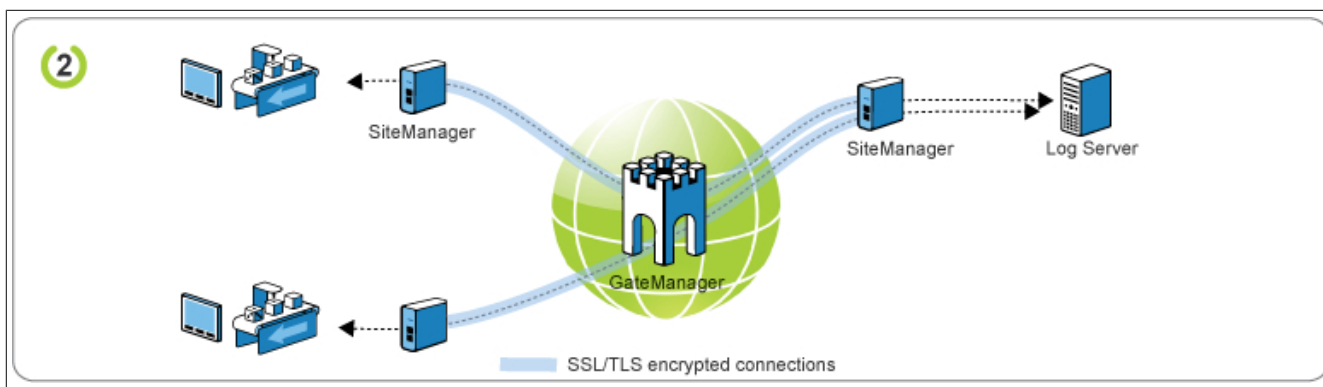


This is the primary function of the B&R Industry solution. The purpose is to provide multiple technicians programming access to devices at multiple sites.

Who has access to what, is centrally controlled by the technician's LinkManager account on the GateManager, on which all access is logged as well.

No fixed or public IP addresses are needed, and all connections by SiteManagers and LinkManagers use standard web-based SSL/TLS protocols, thus making the solution extremely firewall friendly.

#### 8.1.2 Remote monitoring - Secure data logging (between 2 SiteManagers)



This function allows static connections between devices that are behind SiteManagers at different locations. This is an easy method to e.g. allow a log server to collect data from devices, and is typically used for utility installations.

The setup can be based on either a Device Relay or a Server Relay, depending on whether the devices should push log data to the server or the server should collect them from the device. The setup is based on virtual IP addresses, which means that subnet conflicts will not occur. In fact all devices could have the same IP address.

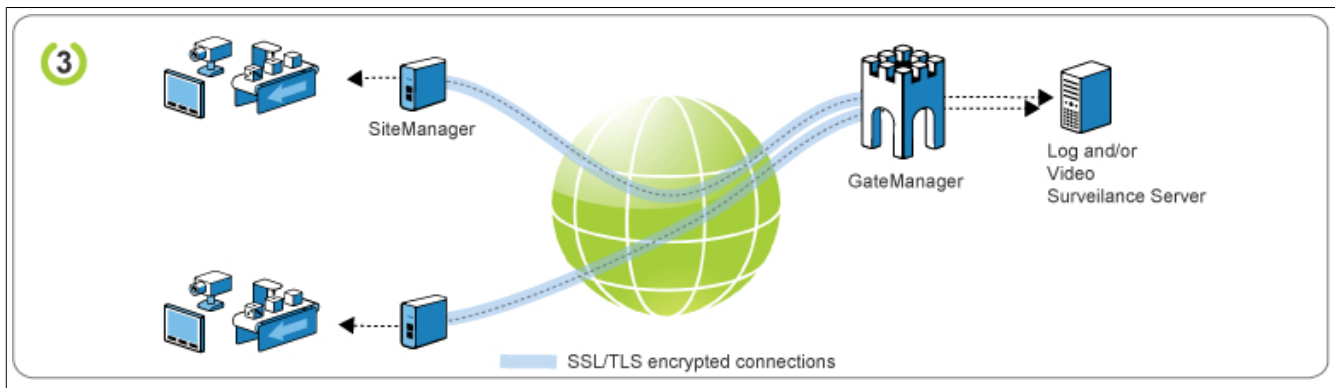
Just like the solution above, this setup is only used web-based SSL/TLS connections, which means it is extremely firewall friendly.

#### Information:

For the implementation of video streaming or full tunneling, see the solutions from the following sections: ["Remote monitoring - For secure data logging" on page 53](#) and ["Direct Internet access - For data logging and video surveillance" on page 53](#)



### 8.1.3 Remote monitoring - For secure data logging

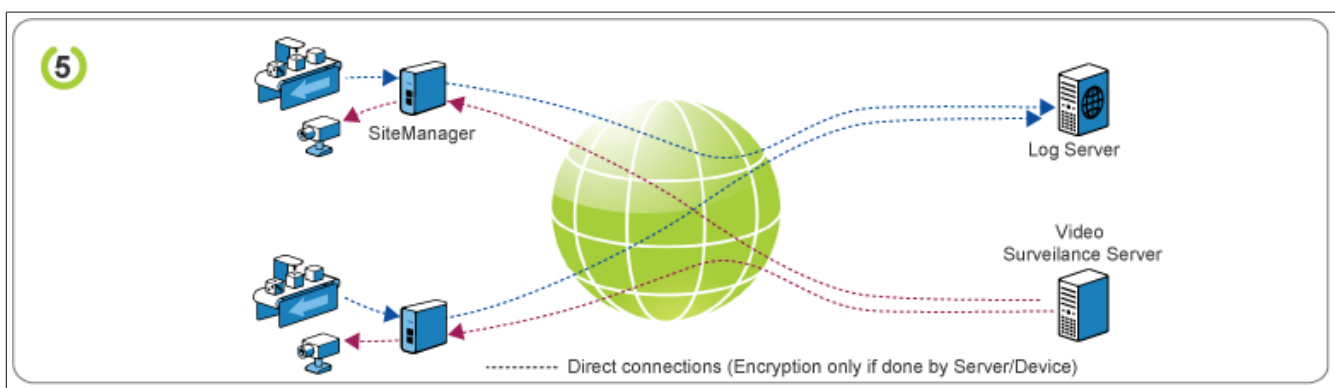


This setup uses the same relay principles as solution 2, but is based on the GateManager server being installed at the same site as the server.

The advantage is that relay connections for bandwidth intensive data, such as video can now be used. Similar to a VPN concentrator, the GateManager server needs to be accessible on a public IP address, but the server itself could be placed in a DMZ or behind a firewall that uses an NAT for the connection to the GateManager.

As above, the setup is based on virtual IP addresses, which means that subnet conflicts will not occur and all devices could have the same IP address. The solution is based solely on web based SSL/TLS connections, which means it is extremely firewall friendly.

### 8.1.4 Direct Internet access - For data logging and video surveillance



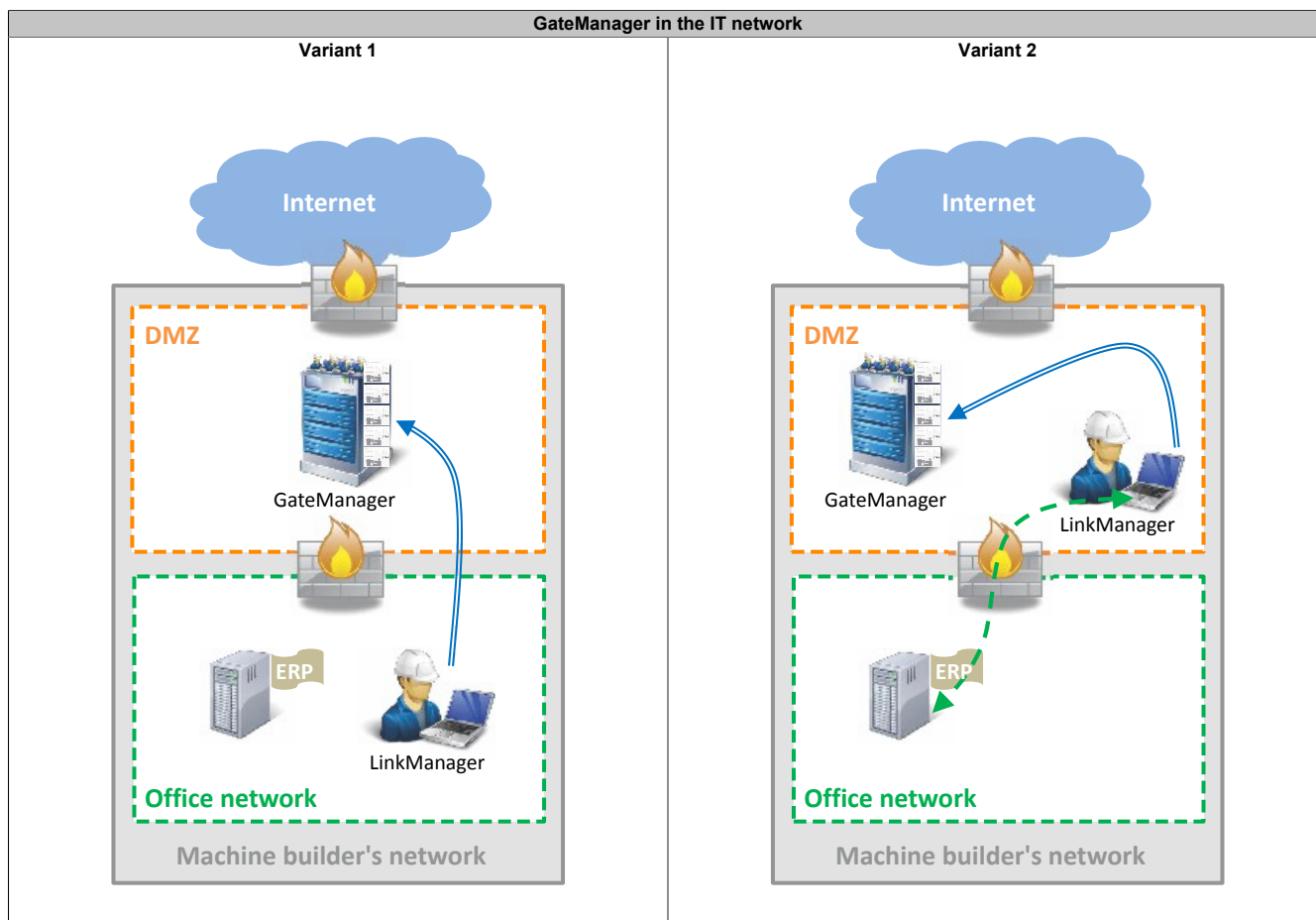
This function is enabled by the SiteManager Forwarding Agent. Basically this allows a device to use the SiteManager as an Internet gateway for sending log data to a web service.

Alternatively, it can be used by a video surveillance system that is connected to the IP address of the SiteManager. This, in turn, forwards the connection request to a defined port on the device. (In order to do this, the SiteManager must be assigned a public IP address; SiteManagers connected via mobile network normally have an Internet agreement with a static IP address.)

## 8.2 End customer scenarios

The operator of the remote maintenance system is usually the machine manufacturer who looks after their end customers and operates the GateManager in a separate IT department. This means that every shipped system/machine has access to the GateManager in order to be able to carry out remote maintenance safely and securely.

Installing the GateManager in a DMZ (separate network zone) is recommended due to IT security concerns. The LinkManager user can then connect through the firewall with the GateManager in the DMZ. Alternatively, the LinkManager user can also be a part of the GateManager DMZ and therefore has access from their PC – via the encrypted VPN tunnel – to the GateManager. The PC of the service technician is therefore in the subnet of the GateManager. Unencrypted communication from the same PC to the office network is verified by the firewall of the DMZ.

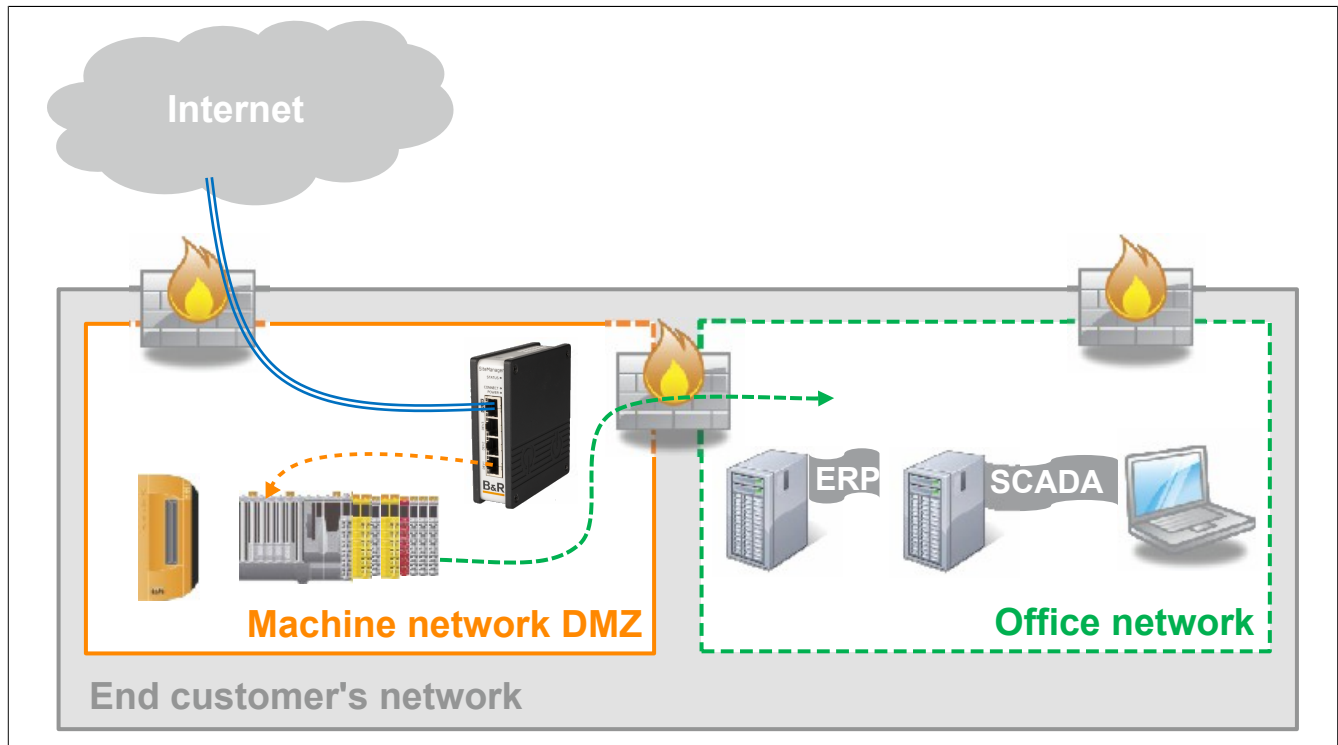


Generally, it should be noted that the machine manufacturer usually defines the device agents for the SiteManager and integrates the SiteManager into the end customer's machine network. Usually the end customer has a machine network and an office network. Often in doing so, devices from the machine network must access the office network in order to receive recipe and order data. Which of the following scenarios can be carried out strongly depends on the end customer's available IT infrastructure. Below, some scenarios are outlined that present an option for integrating the SiteManager into a factory or machine network.

### 8.2.1 SiteManager and machine in an isolated network

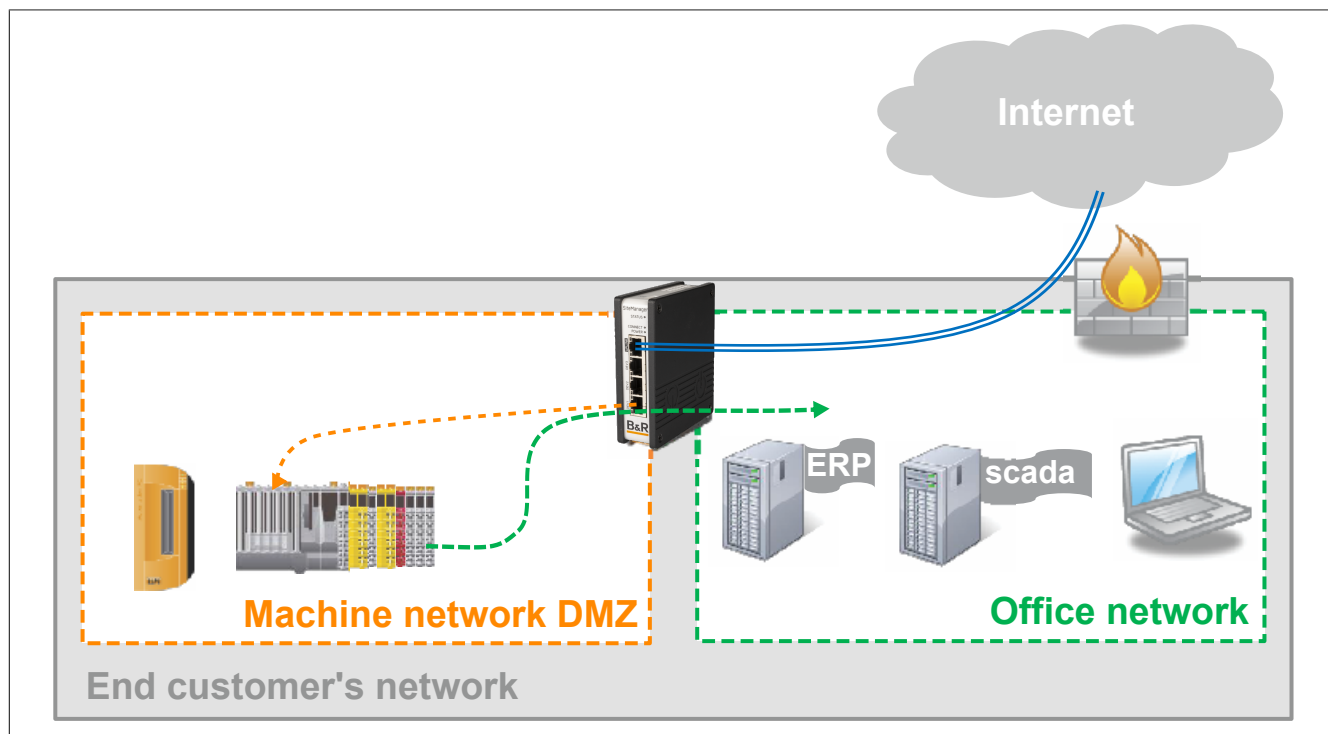
Both networks are separated from each other by a firewall. Only selected machines gain access to the office network. The data traffic of the machine network and SiteManager that goes to and from the Internet is handled by a firewall.

Corresponding device agents must be defined by the machine manufacturer for communication through the SiteManager's firewall. Communication from remote maintenance access is only possible via the device agents. A separate web proxy of the end customer could be used in order to provide the SiteManager with access to the GateManager.



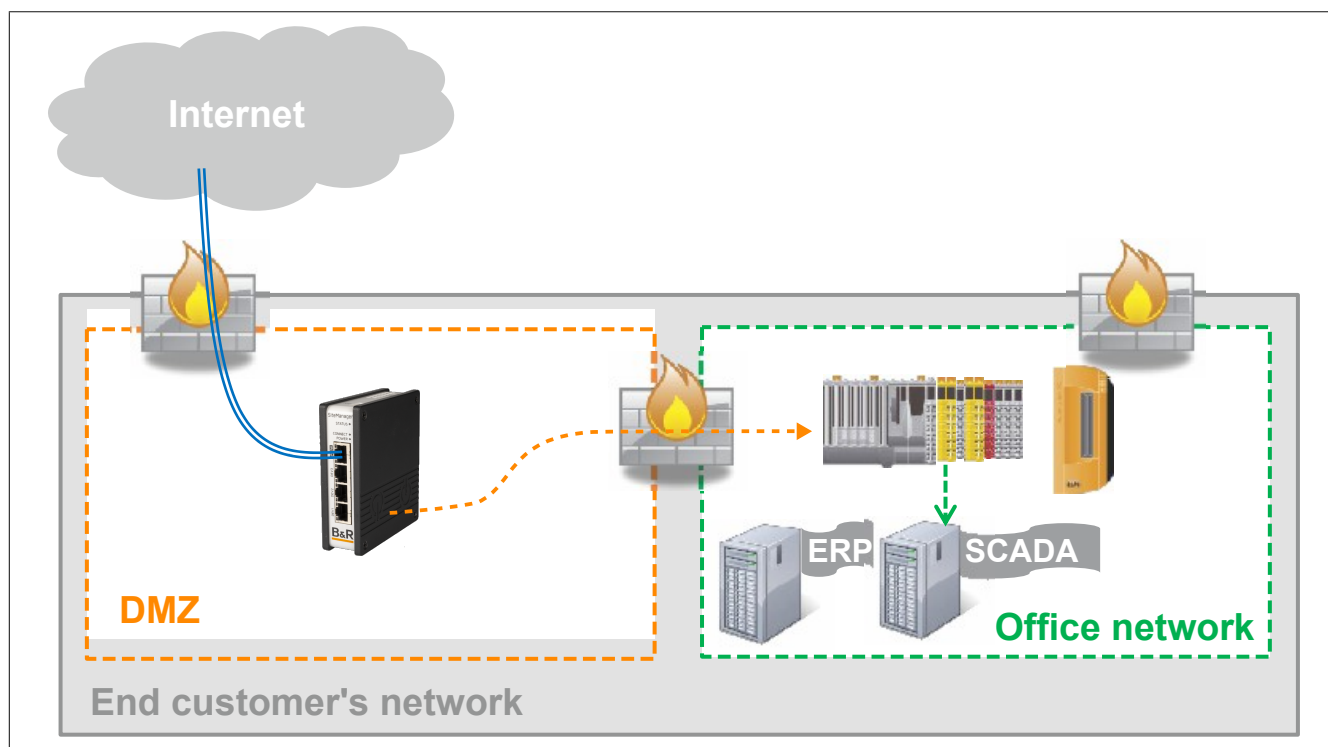
### 8.2.2 Machine network isolated behind DMZ and SiteManager

Machine network and office network are separated by SiteManager. It is possible for a LinkManager user to access the devices in the machine network – but not the office network – through the device agents. Only selected machines gain access to the office network. This can be achieved through static routes or port forwarding on the SiteManager.



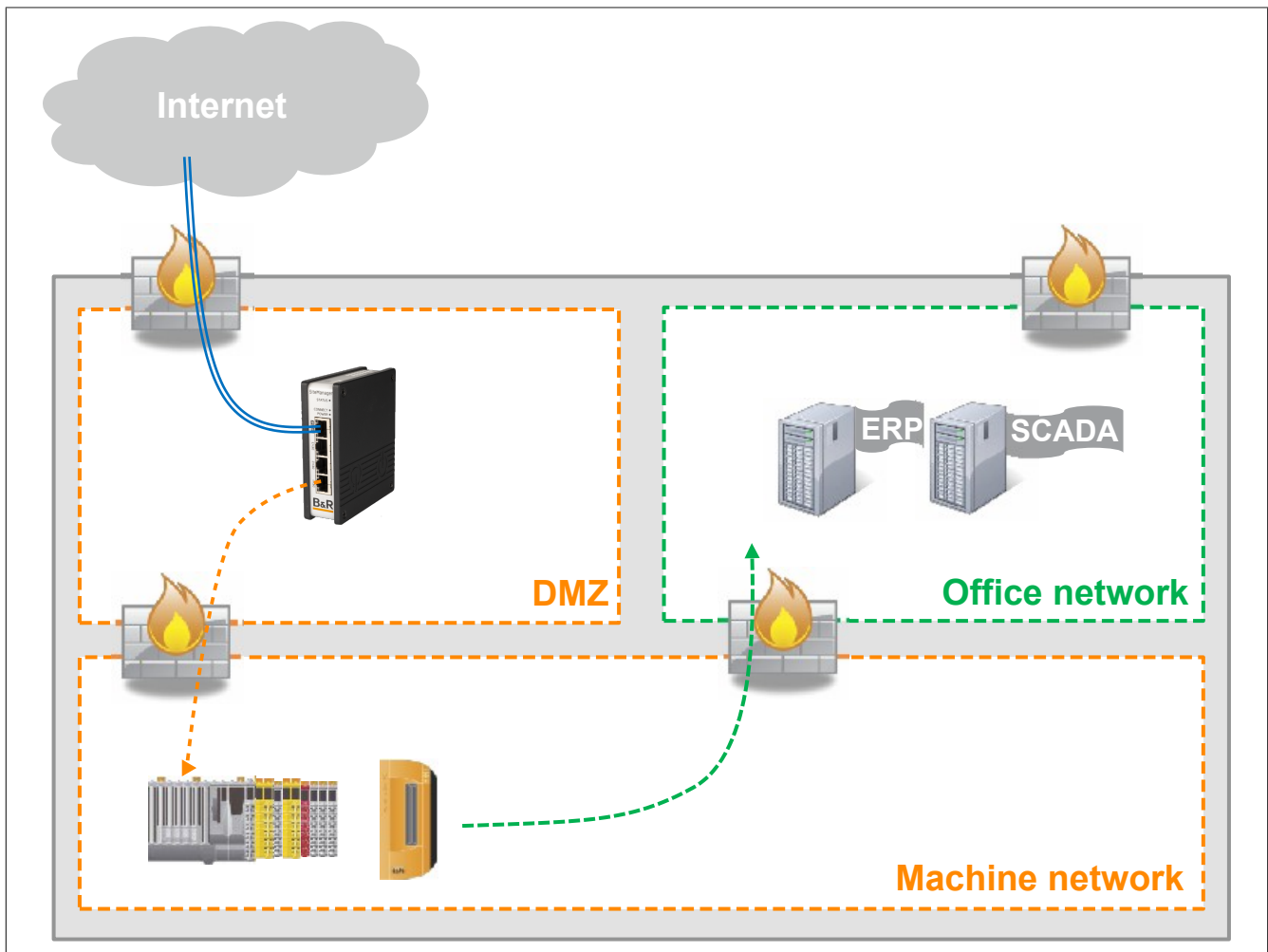
### 8.2.3 SiteManager isolated in a separate DMZ

In this scenario the office and machine networks are not separated from each other. The SiteManager is integrated in its own DMZ. Any data traffic from the SiteManager to the machines must pass a firewall. Since the endpoint of the VPN connection is located in the DMZ, an application firewall located between the DMZ and office network can now view the data traffic and check it for malicious software. In addition, this firewall can restrict access to the office network, making unwanted access impossible if there are potential configuration errors in the device agents.



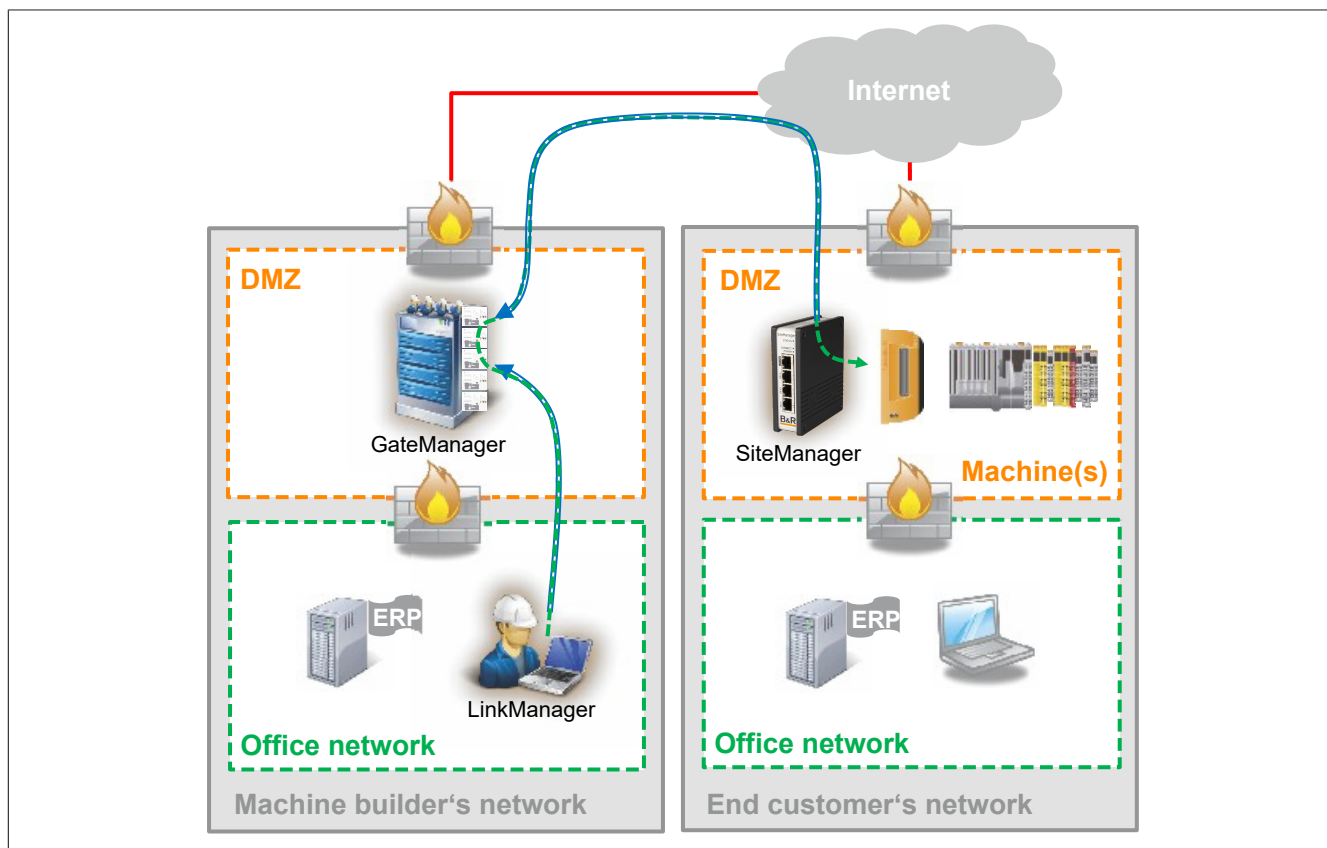
### 8.2.4 SiteManager and machine in separate networks

In this scenario the office and machine networks are separated and the SiteManager is installed in a separate DMZ. Even here the endpoint of the VPN connection lies in a DMZ and the data stream from the SiteManager into the machine network can be verified by the application firewall. The SiteManager cannot access devices on the office network (e.g. ERP system) because the office network is not integrated in the machine network. This scenario offers the most security of the use cases listed here.



### 8.2.5 Remote maintenance - Complete scenario

The figure illustrates a possible implementation scenario. The GateManager is installed in its own DMZ on the machine builder side. Service technicians connect from the office network via the LinkManager to the DMZ. The firewall between the office network and DMZ regulates who is permitted to access the DMZ. A similar structure is selected on the end customer and machine side. Here, the SiteManager and the machine network are separated by a separate DMZ from the office network of the end customer. The firewall between the networks is used to control access.



## 8.3 Establishing a connection with FTP

### Introduction

Only passive mode is used to connect to the FTP server. Errors can occur in active mode when using a firewall and NAT. Since SiteManager has a firewall, the ports required for FTP must first be enabled. For example, communication with the FTP server takes place via port 21. The data transfer takes place at random via a port between 49152 and 65535. This area must therefore also be enabled.

### 8.3.1 FTP via SiteManager

#### Example setup

##### Controller and software used

- X20CP3685
- Automation Runtime I4.33

##### Configuration FTP client

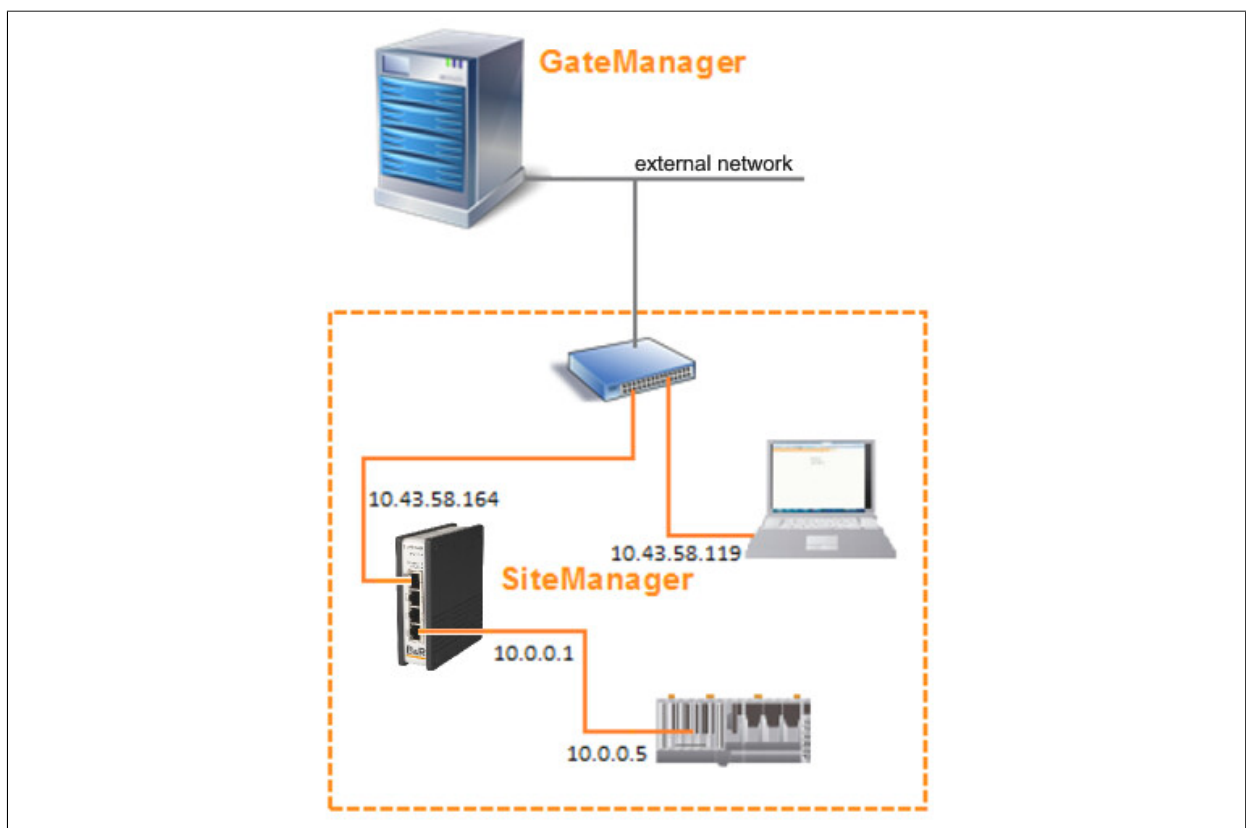
- IP address: 10.43.58.119  
Subnet mask: 255.255.255.0

##### Configuration SiteManager

- External IP address (UPLINK): 10.43.58.164  
Subnet mask: 255.255.255.0
- Internal IP address (DEV): 10.0.0.1  
Subnet mask: 255.255.255.0

##### Configuration FTP server

- IP address (ETH): 10.0.0.5  
Subnet mask: 255.255.255.0



## Forwarding agent

The forwarding agent is created as a **custom (advanced)** device type.

There are 2 ways to use the forwarding agent:

- 1) Permitting a device to access another interface
- 2) Allowing a connection to a device via the uplink port

This agent provides a fast way to access a device on the device page via the UPLINK IP address and vice versa. The function of the SiteManager corresponds to that of a router. Only the ports specified in the forwarding agent are accessible. Multiple forwarding agents can be active at the same time, each of which can contain up to 10 rules.

If the forwarding and routing agents are configured correctly, they are always enabled, regardless of Device Manager or Internet connection. They do not have to be activated via a LinkManager connection. The forwarding and routing agents are not displayed in GateManager or LinkManager.

## Rule format

Each forwarding rule must be created from a combination of the following elements:

```
[#][?][[IN_IFACE*][LOCAL_IP]:][PROTOCOL:][SOURCE_IP[/MASK]:][NAT_PORT]>[>]
[OUT_IFACE*]:]TARGET[/MASK][:TARGET_PORT]
```

### Information:

**Spaces are not permitted in the rule.**

#### Parameter

- ⇒ #  
A "#" at the beginning of the rule indicates that it is deactivated.
- ⇒ ?  
A rule introduced with "?" is optional. Errors caused by this rule are not treated as serious.
- ⇒ IN\_IFACE / LOCAL\_IP  
This specifies the incoming interface or optionally the local IP address or alias for the connection.
- ⇒ PROTOCOL  
Specifies the network protocol from TCP, UDP or ANY. The standard value for this element is TCP. If ANY is used in a rule with NAT\_PORT or TARGET\_PORT, this corresponds to "TCP and UDP", otherwise it corresponds to "any IP protocol".
- ⇒ SOURCE\_IP  
Specifies either a source address or a subnet filter as a rule.
- ⇒ NAT\_PORT  
Specifies the target port or port range for port forwarding to which IN\_IFACE is directed. Port forwarding means that the traffic addressed to a specific port or port range of a SiteManager interface is translated and forwarded to a specific external destination.

### Information:

**When a port forwarding rule is added for TCP port 443, this disables access to the SiteManager web-based user interface from the rule's incoming interface. The web-based user interface can be accessed at any time from another interface, via Appliance Launcher, the RemoteManager or GateManager (if remotely controlled).**

- ⇒ >> or >  
No source translation is used for ">".  
With ">>", the source NAT translation is applied to the traffic forwarded by this rule, making SiteManager the source of the forwarded traffic.
- ⇒ OUT\_IFACE:  
Specifies the outgoing interface for the connection.
- ⇒ TARGET  
Specifies the permissible IP address or subnet for the connection to the external area from SiteManager.



## ⇒ TARGET\_PORT

If NAT\_PORT is set, TARGET\_PORT specifies the destination port or port range for the forwarded traffic.  
If TARGET\_PORT is not set, the target port corresponds to NAT\_PORT.

**Information:**

**If a port range is specified in NAT\_PORT, do not specify a port range here. Otherwise, the TARGET\_PORT part specifies the permitted target port number (n) on the target system.**

**Optional parameters**

## • +TUP

If this option is set, the forwarding agent applies source NAT to all connections that are output via an uplink port (from a device on a DEV interface), regardless of settings ">" or ">>" in the forwarding rules. This means that the target system will see the SiteManager UPLINK IP address as the source address and not the original device IP address. This option is usually activated when outbound forwarding rules (from DEV to UPLINK) are created. If this parameter is deactivated, the static routes on the target system pointing to the UPLINK IP address probably need to be configured so that the target system can identify the gateway back to the device.

## • +TDEV

If this option is set, the forwarding agent applies source NAT to all connections that are output via a DEV interface (from a system on an UPLINK port), regardless of settings ">" or ">>" in the forwarding rules. This means that the target device sees the SiteManager DEV IP address as the source address instead of the IP address of the original system. This option is usually enabled when creating incoming forwarding rules (from UPLINK to DEV).

**8.3.2 Settings in SiteManager****Creating the required agents**

GateManager is opened in the menu bar and then the agents. New agents can be created, edited, disabled, enabled and deleted here. 2 agents must be created and configured for this setup.

**Agent No. 1 configuration**

- Device name: e.g. Forwarding agent 1
- Device: CUSTOM (advanced)
- Type: Forwarding
- Forwarding rule: UPLINK\*:TCP:21>>DEV1:10.0.0.5

Forwarding Agent 1	CUSTOM (Advanced) ▼	Forwarding ▼	UPLINK*:TCP:21>>DEV1:10.0.0.5
--------------------	---------------------	--------------	-------------------------------

This rule automatically forwards all TCP packets sent from the UPLINK port to the SiteManager (10.43.58.164) via port 21 to the FTP server (10.0.0.5).

**Agent No. 2 configuration**

- Device name: e.g. Forwarding agent 2
- Device: CUSTOM (advanced)
- Type: Forwarding
- Forwarding rule: UPLINK\*:TCP:49152-65535>>DEV1:10.0.0.5

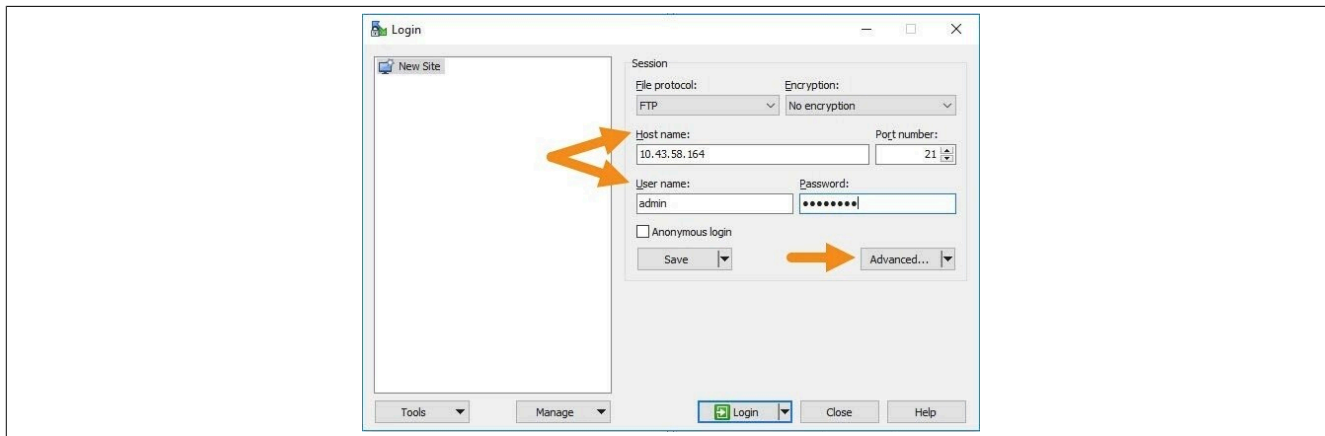
Forwarding Agent 2	CUSTOM (Advanced) ▼	Forwarding ▼	UPLINK*:TCP:49152-65535>>DEV1:10.0.0.5
--------------------	---------------------	--------------	--

This rule corresponds to the first, but only TCP packets sent to SiteManager (10.43.58.164) via ports in the range from 49152 to 65535 are forwarded.

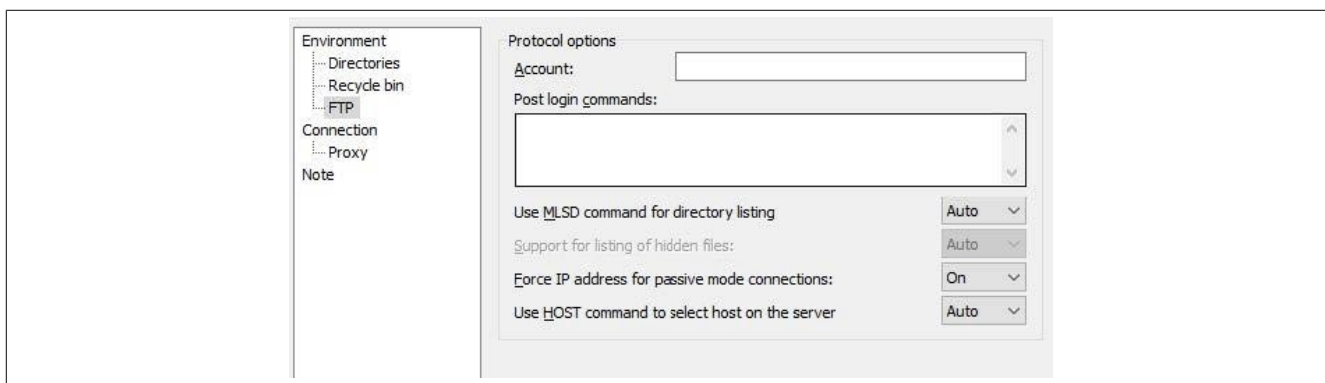
### 8.3.3 Creating a connection with WinSCP

This example refers to Version 5.9.6 Build 7601 of the WinSCP.

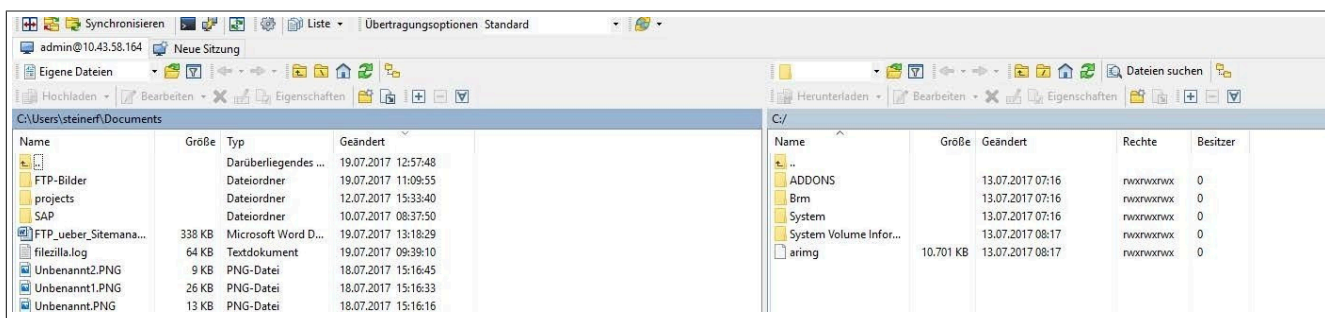
After starting the client, a login window opens in which the IP address of the SiteManager and the login data of the FTP server are entered.



Clicking button "Advanced" opens a new window from which submenu "FTP" can be selected via menu tree "Environment". Here, the settings are configured according to the following figure.



The entries must then be confirmed, the settings saved and a name assigned for the connection. After confirming any existing password for the user, the connection to the FTP server is established.



## 9 Error correction

Error correction for access from the SiteManager to the GateManager via a company intranet

The following sections can be used to verify from the PC whether a SiteManager can access the GateManager through the corporate firewall.

### 9.1 Testing GateManager access from a PC

The SiteManager attempts to access the Internet by successively trying the following connection methods from its uplink port:

- 1) Port 11444 (verification: <https://gm01.br-automation.com:11144>)
- 2) Port 443 with HTTPS/TLS (verification: <https://gm01.br-automation.com>)
- 3) Port 80 with TLS over HTTP (verification: <https://gm01.br-automation.com:80>)
- 4) TLS via web proxy

If the above verification links are clicked or entered in a web browser, at least one of the links should provide this result:



This view should appear after selecting "Continue to this website":



If none of the links opens up the views above, it may be due to the following reasons:

1. A firewall is blocking TLS access and only permitting plain text/html (i.e. <http://...> is supported, <https://...> is not). Special rules may need to be set up in the firewall for the PC. This can be solved by approving the IP address, MAC address, DNS name of the PC or the PC itself on a local MS Directory Services server.
2. Internet access requires a web proxy that is not configured on the PC from which the connection is being attempted. This is normally provided by the DHCP server but may also need to be configured manually (Tools → Internet options → Connections → LAN settings → Proxy server in MS Internet Explorer).

If all of the above have been checked and the LinkManager Mobile login screen is still not displayed on the PC, connecting through the SiteManager will not be possible either. In this case, the IT administrator must be contacted.

## 9.2 Connection from PC possible, but not from SiteManager

### 9.2.1 Basic questions

- **Ethernet cable not connected properly**

Incorrectly connected cables are a common cause of error. Verify that the network over which the SiteManager should access the Internet is connected to the SiteManager uplink port, and verify that the Ethernet port is connected (the green-yellow LEDs on the Ethernet port itself are lit).

- **Problems configuring the Uplink1 IP address**

Ensure that the SiteManager has an IP address that matches the network that should be used to access the Internet.

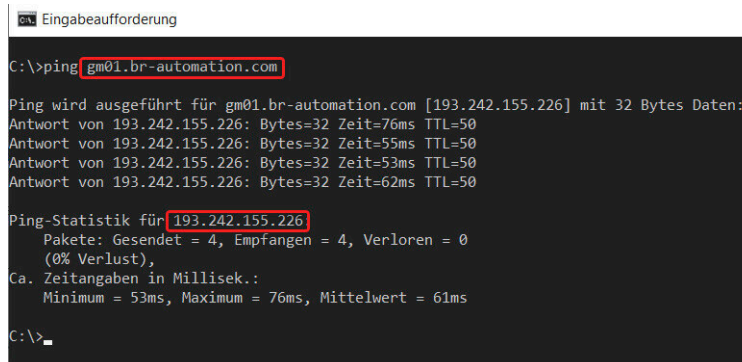
**If the Uplink1 IP address is assigned via DHCP**, check whether an address has actually been assigned. Connect the PC to the DEV network and use Secomea Appliance Launcher to search for the SiteManager and verify the assigned uplink IP address. Alternatively, the lease table of the DHCP server can be checked. Also try to ping this IP address from a PC in the same network.

**If the Uplink1 IP address is statically configured**, check that it matches the subnet of the network to which it is connected. Also check whether the subnet mask matches the subnet class and whether the default gateway is defined as the router providing Internet access. Try to ping the IP address from a PC on the same network. A good test is to access the SiteManager web-based user interface from the Uplink1 or DEV page (enter "https://" in the web browser before the IP address, default login/password is "admin/admin"), and use the ping function in SiteManager menu Status → ping/trace to ping the Internet gateway.

- **DNS problem**

If the DNS name of the GateManager server is used in the SiteManager configuration, e.g. "gm01.br-automation.com", it may not be resolved to the IP address correctly and should be changed to the IP address (menu GateManager → General).

Open the command prompt and ping the DNS name of the GateManager so that the IP address (193.242.155.112) is resolved:



```

C:\>ping gm01.br-automation.com

Ping wird ausgeführt für gm01.br-automation.com [193.242.155.226] mit 32 Bytes Daten:
Antwort von 193.242.155.226: Bytes=32 Zeit=76ms TTL=50
Antwort von 193.242.155.226: Bytes=32 Zeit=55ms TTL=50
Antwort von 193.242.155.226: Bytes=32 Zeit=53ms TTL=50
Antwort von 193.242.155.226: Bytes=32 Zeit=62ms TTL=50

Ping-Statistik für 193.242.155.226:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 53ms, Maximum = 76ms, Mittelwert = 61ms

C:\>_
  
```

The SiteManager supports the use of a DNS name as a GateManager server destination, but it is recommended to use the IP address in order not to depend on a DNS server in the network.

## 9.2.2 Web proxy issues

A web proxy is often used to validate Internet access. The SiteManager is designed such that the Internet and the GateManager can be accessed via a web proxy.

If the SiteManager obtains its uplink IP address through DHCP, it automatically considers the default gateway as a web proxy, including Web Proxy Auto-Discovery (WPAD). It thus automatically extracts the information from the PAC file distributed by the DHCP server.

However, there are 2 scenarios that require manual configuration of the web proxy in the SiteManager configuration menu:

- 1) If the SiteManager obtains its IP address via DHCP, but the web proxy requires entry of a password.
- 2) If the SiteManager does not obtain its uplink IP address through DHCP (but is statically configured), SiteManager cannot automatically detect the web proxy settings.

These settings must therefore be entered manually in the SiteManager user interface under GateManager → General.

The screenshot shows the SiteManager web interface. The top navigation bar includes links for Maintenance, Setup, System, GateManager, Routing, DCM, Maintenance, Status, Log, and HELP. The 'GateManager' tab is active, and the 'General' sub-tab is selected. The main heading is 'GateManager Settings'. Below this, it states 'GateManager not connected.' with a green refresh icon. The 'Remote Management' dropdown is set to 'Enabled'. There are three mandatory fields (marked with an asterisk): 'GateManager Address' (trialgm.br-automation.com), 'Domain Token' (productmanagement), and 'Appliance Name' (070823\_4G). A red box highlights the 'Web-proxy Address', 'Web-proxy Account', and 'Web-proxy Password' fields. Below these is the 'Connection Watchdog' dropdown set to 'Reset modem only'. A legend indicates that an asterisk (\*) denotes a mandatory field. At the bottom are 'Save', 'More >>', and 'Connect' buttons.

For detailed information about configuring the web proxy settings, see the SiteManager help documentation.

It should be noted, for example, that the URL path to the WPAD file can be set manually in the Web Proxy Address field, which is useful if no web proxy information has been obtained from a DHCP server.

If an NTLM-based web proxy is used, the account can also be entered in the Web proxy account field in the format "DOMAIN\USER".

### Information:

It is possible that the LinkManager gains access to the GateManager although the NTLM account is not configured in the LinkManager. This may be due to the fact that the PC itself has already been permitted by the proxy.

### 9.2.3 Other possibilities

If the SiteManager is configured correctly, check the following on the network.

These things must usually be checked by local IT administrators and definitely require someone from IT to make changes:

- 1) Does the firewall need to enter an exception for the source IP address of an unknown device into the firewall to access the Internet?  
If so, enter the IP address of the SiteManager Uplink1 port.
- 2) Does the firewall require an exception for a device's MAC address to be entered into the firewall to access the Internet?  
If so, enter the MAC address of the SiteManager's uplink1 port. It is important to note that the Uplink1 MAC address is usually one higher than the DEV1 MAC address, which is also the SiteManager serial number. If Appliance Launcher detects 00:05:B6:00:97:6C on the DEV interface, for example, the uplink MAC address is 00:05:B6:00:97:6D. Check the MAC address by checking the network's DHCP lease table, or ping uplink1 and check the ARP cache.
- 3) Does the firewall or proxy require that a device's DNS be classified as trusted (e.g. checked by reverse lookup)?  
Since the SiteManager is not a Windows PC, a special exception may need to be made.
- 4) Must an exception be entered in the firewall for the destination IP that a device is trying to access?  
Enter the IP address of the GateManager server.
- 5) Does the firewall require the use of DNS names that are resolved locally?  
In this case, the DNS name of the GateManager must be entered on the DNS server (e.g. "gm02.sec-omea.com" and specified with its IP address 193.242.155.112). It must next be ensured that the SiteManager is configured with the IP address of the DNS server. This is usually distributed automatically via DHCP but must be entered manually for the Uplink1 port if it is configured with a static IP address.
- 6) If the firewall is configured to NOT tolerate "rekey" in a TLS session, the SiteManager may be rejected if the firewall did not catch the creation of the original session. This is because the SiteManager uses rekeying when connecting to a GateManager 4x server; the firewall therefore cannot use a cached session ID. The log messages of the firewall can also be checked for this (if enabled). On a Fortinet firewall, for example, the message would read "The SSL session was blocked because the session ID was unknown".  
In this case, an exception must be added in the firewall to allow the SiteManager to bypass this check.

#### Information:

**This is not a problem for GateManager 5, but ONLY for SiteManagers connecting to GateManager 4x servers.**

# 10 Standards and certifications

---

## SiteManager



### Declaration of conformity

[Website > Downloads > Industrial IoT > Remote maintenance > SiteManager](#)

# 11 Terminology and abbreviations

---

Abbreviation	Term	Explanation
DMZ	Demilitarized zone	A computer network with controlled safety-related access to the connected servers.
ERP	Enterprise Resource Planning	Usually refers to the software used to plan the deployment of all types of resources available in a company (e.g. SAP).
FQDN	Fully-Qualified Domain Name	A complete computer name that is displayed as a fully qualified domain name (e.g. remote.companyname.com). The FQHN is a unique designation for a specific computer.
SCADA	Supervisory Control and Data Acquisition	Monitoring and controlling technical processes using a computer system.



## 12 Appendix - Discontinued modules

### Information:

The products mentioned in this section are only for reference purposes when already in use.

### 12.1 GateManager - 0RMGM.4260-TP

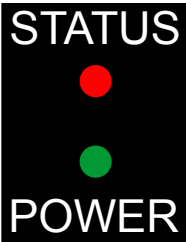
GateManager 0RMGM.4260-TP is no longer available from B&R.

#### 12.1.1 Technical data

Order number	0RMGM.4260-TP
<b>General information</b>	
B&R ID code	0xE8EB
<b>Functionality</b>	
Number of supported SiteManagers	Up to 2000
<b>Mains connection</b>	
Mains input voltage	100 to 240 V
Frequency	50 to 60 Hz
Installed load	36 W
<b>Controller</b>	
Processor	
Type	Dual core Intel Atom™ C2358
Clock frequency	1.7 GHz
Flash	32 GB
DRAM	2 GB
<b>Interfaces</b>	
Interface IF1	
Type	CONSOLE
Variant	1x RJ45 shielded
Line length	Max. 100 m between 2 nodes (segment length)
Transfer rate	Max. 10/100/1000 Mbit/s
Interface IF2	
Type	USB 2.0
Interface IF3	
Type	USB 2.0
Interface IF4	
Type	LAN
Variant	1x RJ45 shielded
Transfer rate	Max. 10/100/1000 Mbit/s
Interface IF5	
Type	WAN
Variant	1x RJ45 shielded
Transfer rate	Max. 10/100/1000 Mbit/s
Interface IF6	
Type	AUX1
Variant	1x RJ45 shielded
Transfer rate	Max. 10/100/1000 Mbit/s
Interface IF7	
Type	AUX2
Variant	1x RJ45 shielded
Transfer rate	Max. 10/100/1000 Mbit/s
<b>Ambient conditions</b>	
Temperature	
Operation	0 to 40°C
<b>Mechanical properties</b>	
Dimensions	
Width	177 mm
Height	44 mm
Depth	145.5 mm
Weight	1.2 kg

Table 13: 0RMGM.4260-TP - Technical data

### 12.1.2 LED status indicators

Figure	LED	Color	Status	Description
	STATUS	Red	Blinking quickly (0.5 s on / 0.5 s off) Blinking slowly (2 s on / 2 s off)	Booting Check the file system. File system verification is performed on every 20th boot (or every 180 days). This check can take up to 5 minutes. <b>Notice!</b> Possible damage to the device! Do not disconnect the module from the power supply while the file system is being checked!
	POWER	Green	On	Power supplied.

### 12.1.3 Operating and connection elements

#### 12.1.3.1 Reset button

The reset button currently has no effect but is reserved for future use.

#### 12.1.3.2 Ethernet interfaces

The interfaces are 10/100/1000 Mbit/s. Use standard Cat. 5 cables (or higher) to connect to a switched network. The interfaces automatically detect crossover connections, so a direct connection to a PC (e.g. for configuration) can be made using a crossover cable or a standard cable.

The WAN interface is used for normal operation. The LAN interface is only for debugging and special configurations.

The two interfaces AUX1 and AUX2 currently have no effect, but are reserved for future use.

#### 12.1.3.3 USB interfaces

USB interfaces are used for backup and restore and/or connecting an optional external USB modem for SMS text message notifications and/or login authentication.

#### Information:

**SMS text message support can be achieved through configuration of an external SMS gateway.**

See also [Configuring SMS gateways on GateManager](#)

The interfaces support a USB 2.0 flash drive that is formatted as FAT 32. The recommended size is 4 GB or more.

#### 12.1.3.4 Power supply

Use the supplied power supply unit on a 100-240 V and 50-60 Hz power outlet.

## 12.2 SiteManager 0RMSM 11x5

### 12.2.1 SiteManager 11x5

These products are identical to the 13x5 models in function and operation.

#### 12.2.1.1 Technical data

Order number	0RMSM1115	0RMSM1135	0RMSM1135.4G	0RMSM1145
General information				
B&R ID code	0xE8E9	0xE8EA	0x29BE	0xE908
Reset button	Yes			
Status LED	Supply voltage Status LinkManager connection	Supply voltage Status LinkManager connection Wireless connection		
Power consumption	Max. 3 W	Max. 5 W		Max. 3 W
Functionality				
Data transfer / Frequency domain				
Integrated broadband modem				
LTE band	-		See 0RMSM1335.4G bands.	-
WCDMA/UMTS	-		See 0RMSM1335.4G bands.	-
WCDMA	-	850 MHz 1900 MHz 2100 MHz	-	
GPRS/EDGE	-	850 MHz 900 MHz 1800 MHz 1900 MHz	B2 (1900) B3 (1800) B5 (850) B8 (900)	-
Integrated Wi-Fi module	-			2400 MHz for client mode
Controller				
Processor				
Type	ARM Cortex-A5			
Clock frequency	563 MHz			
Interfaces				
Interface IF1				
Type	Ethernet UPLINK1			
Variant	Shielded RJ45			
Line length	Max. 100 m between 2 nodes (segment length)			
Transfer rate	Max. 10/100 Mbit/s			
Transfer				
Physical layer	10BASE-T/100BASE-TX			
Half-duplex	Yes			
Full-duplex	Yes			
Autonegotiation	Yes			
Auto-MDI/MDIX	Yes			
Interface IF2				
Type	DEV1			
Variant	Shielded RJ45			
Transfer rate	Max. 10/100 Mbit/s			
Interface IF3				
Type	-	3G/GPRS	4G/3G/GPRS	-
Variant	-	SMA female		-
Transfer rate	-		Downlink: 50 Mbit/s (10 MHz bandwidth) Uplink: 25 Mbit/s (10 MHz bandwidth)	-
Interface IF4				
Type	-			Wi-Fi
Variant	-			RP-SMA female
Electrical properties				
Nominal voltage	12 to 24 VDC			
Degree of protection per EN 60529	IP20			
Ambient conditions				
Temperature				
Operation	-25 to 60°C	-25 to 45°C	-25 to 60°C	-25 to 60°C
Relative humidity				
Operation	5 to 95%			
Storage	5 to 95%			
Transport	5 to 95%			
Mechanical properties				
Material	Aluminum			

Order number	0RMSM1115	0RMSM1135	0RMSM1135.4G	0RMSM1145
Dimensions				
Width	32 mm			
Height	107 mm			
Depth	97 mm			
Weight	0.5 kg			

### 0RMSM1135.4G bands

	LTE bands	WCDMA/UMTS bands
B1 (FDD 2100) IMT	X	X
B2 (FDD 1900) PCS	X	X
B3 (1800 +) DCS	X	
B4 (1700) AWS	X	X
B5 (850) CLR, US, Korea, etc.	X	X
B6 (850) Japan #1		X
B7 (2600) IMT-E	X	
B8 (900) E-GSM	X	X
B12 (700) US	X	
B13 (700c) USMH, LSMH US	X	
B18 (800 or 850?) Japan #4	X	
B19 (800 or 850?) Japan #5	X	X
B20 (800) digital dividend	X	
B25 (1900 b Block)	X	
B26 (850+) extended CLR	X	
B28 (700 APT) APAC	X	
B34 (TDD)	X	
B38 (TDD 2600) IMT-E	X	
B39 (TDD 1900 +) China	X	
B40 (TDD 2300) China	X	
B41 (TDD 2500) BRS/EBS	X	
B66 (TDD)	X	

### 12.2.2 SiteManager 4G - Regional variants

SiteManager 4G - Regional variants are no longer available from B&R.

#### 12.2.2.1 Technical data

#### Information:

**SiteManager variant 1135.4G-xx is available in editions for the following regions: USA, EMEA, Japan and China. Each variant supports dedicated frequencies/bands as well as wireless carriers (SiteManager 0RMSM1135.4G-US will not work with a Verizon SIM card, however). All SiteManager 1135.4G-xx variants also support 3G, in case 4G is not yet available in a specific region.**

Bestellnummer	0RMSM1135.4G-CN	0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
General information				
B&R ID code	0xEE28	0xEE27	0xF241	0xEE26
Reset button	Yes			
Status LED	Supply voltage Status LinkManager connection Wireless connection			
Power consumption	Max. 5 W			
Functionality				
Data transfer / Frequency domain				
Integrated broadband modem				
LTE band	B1 (FDD 2100) IMT B3 (1800 +) DCS B5 (850) CLR, US, Korea, etc. B7 (2600) IMT-E B8 (900) E-GSM B38 (TDD 2600) IMT-E B39 (TDD 1900 +) China B40 (TDD 2300) China B41 (TDD 2500) BRS/EBS	B1 (FDD 2100) IMT B3 (1800 +) DCS B7 (2600) IMT-E B8 (900) E-GSM B20 (800) digital dividend B38 (TDD 2600) IMT-E B40 (TDD 2300) China	B1 (FDD 2100) IMT B3 (1800 +) DCS B8 (900) E-GSM B18 (800 or 850?) Japan #4 B19 (800 or 850?) Japan #5	B2 (FDD 1900) PCS B4 (1700) AWS B5 (850) CLR, US, Korea, etc. B17 (700bc) USMH, LSMH US
WCDMA/UMTS	B1 (FDD 2100) IMT B8 (900) E-GSM	B1 (2100) IMT B8 (900) E-GSM	B1 (2100) IMT B6 (850) Japan #1 B8 (900) E-GSM	B2 (1900) PCS B5 (850) CLR
GPRS/EDGE	B3 (1800) B8 (900)	B3 (1800) B8 (900)		-

Tabelle 14: 0RMSM1135.4G-CN, 0RMSM1135.4G-EU, 0RMSM1135.4G-JP, 0RMSM1135.4G-US - Technische Daten

Bestellnummer	0RMSM1135.4G-CN	0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
<b>Controller</b>				
Processor				
Type			ARM Cortex-A5	
Clock frequency			563 MHz	
<b>Interfaces</b>				
Interface IF1				
Type			Ethernet UPLINK1	
Variant			Shielded RJ45	
Line length			Max. 100 m between 2 nodes (segment length)	
Transfer rate			Max. 10/100 Mbit/s	
Transfer				
Physical layer			10BASE-T/100BASE-TX	
Half-duplex			Yes	
Full-duplex			Yes	
Autonegotiation			Yes	
Auto-MDI/MDIX	Yes		Yes	
Interface IF2				
Type			DEV1	
Variant			Shielded RJ45	
Transfer rate			Max. 10/100 Mbit/s	
Interface IF3				
Type			4G/3G/GPRS	
Variant			SMA female	
Transfer rate			Downlink: 50 Mbit/s (10 MHz bandwidth) Uplink: 25 Mbit/s (10 MHz bandwidth)	
<b>Electrical properties</b>				
Nominal voltage			12 to 24 VDC	
<b>Operating conditions</b>				
Degree of protection per EN 60529			IP20	
<b>Ambient conditions</b>				
Temperature				
Operation			-25 to 45°C	
Relative humidity				
Operation			5 to 95%	
Storage			5 to 95%	
Transport			5 to 95%	
<b>Mechanical properties</b>				
Material			Aluminum	
Dimensions				
Width			32 mm	
Height			107 mm	
Depth			97 mm	
Weight			0.5 kg	

Tabelle 14: 0RMSM1135.4G-CN, 0RMSM1135.4G-EU, 0RMSM1135.4G-JP, 0RMSM1135.4G-US - Technische Daten

**LTE bands**

	0RMSM1135.4G-CN	0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
B1 (FDD 2100) IMT	X	X	X	
B2 (FDD 1900) PCS				X
B3 (1800 +) DCS	X	X	X	
B4 (1700) AWS				X
B5 (850) CLR, US, Korea, etc.	X			X
B7 (2600) IMT-E	X	X		
B8 (900) E-GSM	X	X	X	
B17 (700bc) USMH, LSMH US				x
B18 (800 or 850?) Japan #4			X	
B19 (800 or 850?) Japan #5			X	
B20 (800) digital dividend		X		
B38 (TDD 2600) IMT-E	X	X		
B39 (TDD 1900 +) China	X			
B40 (TDD 2300) China	X	X		
B41 (TDD 2500) BRS/EBIS	X		X	

**WCDMA/UMTS bands**

Band	0RMSM1135.4G-CN	0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
B1 (FDD 2100) IMT	X	X	X	
B2 (FDD 1900) PCS				X
B5 (850) CLR, US, Korea, etc.				X
B6 (850) Japan #1			X	
B8 (900) E-GSM	X	X	X	